

MICHIGAN STATE
UNIVERSITY
Beta Presentation

**Next Generation Malware Analysis
System**

The Capstone Experience

Team Proofpoint

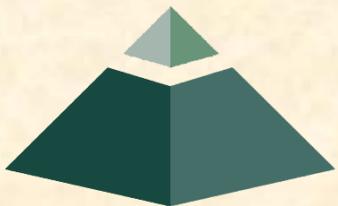
Brad Doherty

Crystal Lewis

Yash Patel

Graham Thomas

George Zhao



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

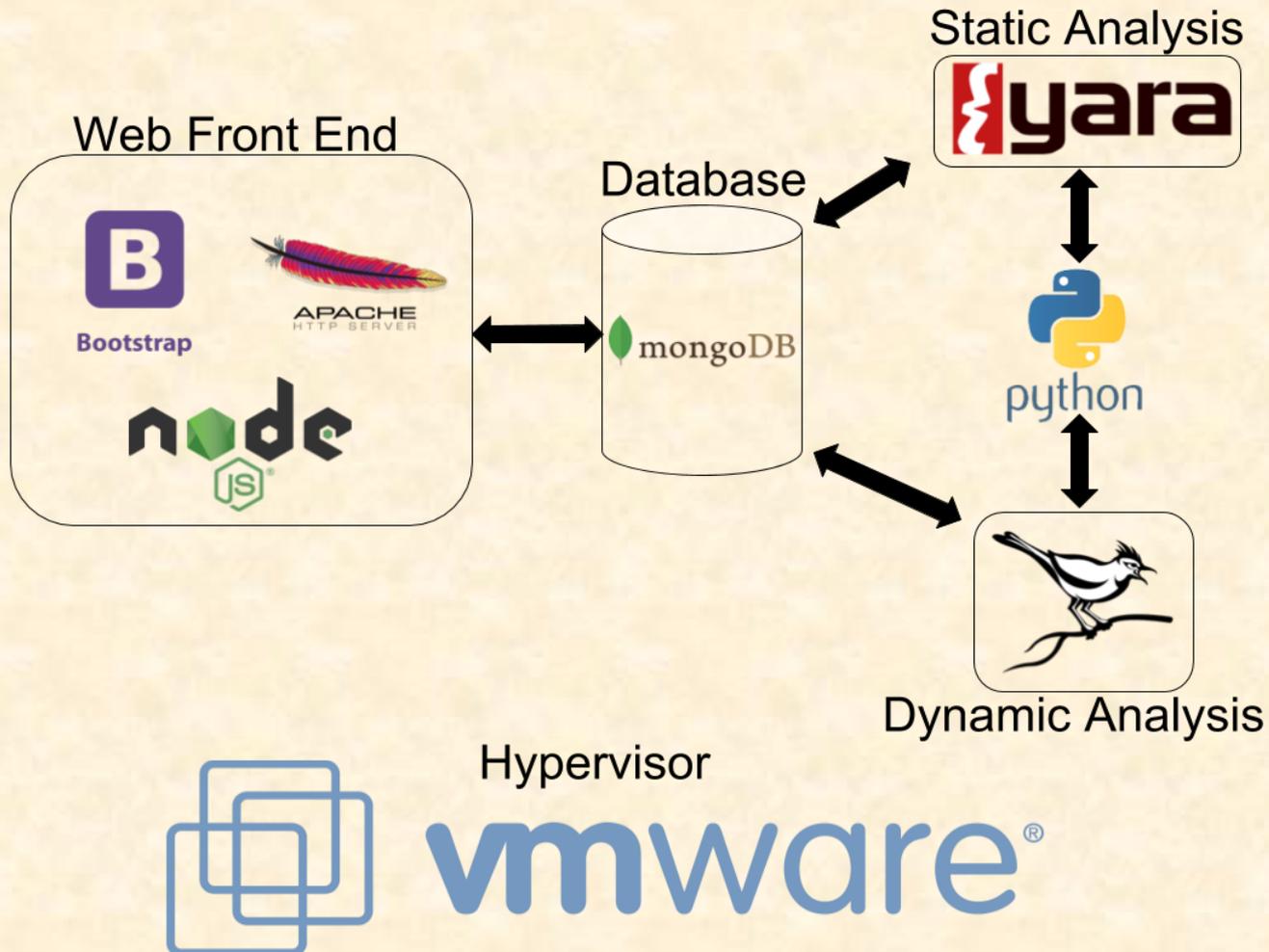
Department of Computer Science and Engineering
Michigan State University
Spring 2018

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

Malware Analysis Dashboard

Dashboard

415 Clusters of Malware

Average Static Analysis Time 00:00:01.788

1,106 Total Files Analyzed

Current Queue of Cuckoo

Position	TaskID	File Name
1	150	65F31AE9563F9AAF782941FFA67BA46260A21CBA0B0C9968545EADI
2	151	955626A5C3A583353A135DD3737A0E0DCAAC94CA5BE09CC7AE84C
3	152	D49BD707B4D52C21F1CE97961C965D47269BC6B77EE9F2C1AA59A11
4	153	83DA562775023AF437C818DAFA4C70B91E6252A802D63B86003244
5	154	1527FC7C5F13E4D2FC1BF8DA7D68C1E5D2FEDF6960FB6E68BC7056C

View More

Top 5 Yara Rules Matched

YARA Rule	Count
Str_Win32_Winsock2_Library	534
No Matches	251
RijnDael_AES_CHAR	241
RijnDael_AES_LONG	241
XMRIG_Miner	231

View More

22.7% of files analyzed do not match a YARA Rule

77.3% of files analyzed match one or more YARA Rule

View More Known Files

View More Flagged Files

FLAGGED FILES

- 65F31AE9563F9AAF782941FFA67BA...
- 955626A5C3A583353A135DD3737A0...
- D49BD707B4D52C21F1CE97961C965...
- 83DA562775023AF437C818DAFA4C7...
- 1527FC7C5F13E4D2FC1BF8DA7D68C...
- 3EDB4F6CFE6A9CC12F599B78051C6...
- E722DAB92F4B85A3FFF8CA5158CB6...
- 2A225193A481E53920CF8351764F4...
- FBE2D7D678047B0BC43E78B09B36...

And 242 more files...

KNOWN MALWARE FILES

- 69CEFFE306948C50094B45D104431...
- 09CBE28B18E9DE87DE93E7E58EFAE...
- C6A13AFC5831096B0CCB54FBB2B3...
- 48678EC3D22C571774ACE303C4C7...
- 58B010F35B2616FACF99EEB108732B...
- 69760CD6A58F79558443BA6FCE64...
- 973DOB8382AF4504E8F709E1BC605...
- 8632A3DDE098D2C9CCCEBF4EFCBD...
- B9D1A0998496A9B34AE739BDF585...

And 846 more files...

All Malware Files Table

SID	File Name	File Type	# of YARA Matches	Flagged?
1	65F31AE9563F9AAF782941FFA67BA46260A21CBA0B0C9968545EADDEF4CE70E7	PE32 executable (GUI) Intel 80386, for MS Windows	0	Yes
2	955626A5C3A58335A135DD3737A0E0DCAAC94CA8B609CC7AE84CCF5B461ACE	PE32 executable (GUI) Intel 80386, for MS Windows	0	Yes
3	D49BD707B4D52C21F1CE97961C965D47269BC6B7EE9F2C1AA59A11AF8F39C3	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	69CEFFE306948C50094B45D104431166AFB977AD75DA89F315B23E7EFBC08FB	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	2	No
7	09CBE28B18E9DE87DE93E7E58EFAED5C7B4CE36315068EE6A4E004443399B9E3	PE32 executable (GUI) Intel 80386, for MS Windows	36	No
8	C6A13AFC583109680CCB54FB2B3D14E4BA08E9C7A363C884B1383C5EE81FAA	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows	4	No
9	48678EC33D22C571774ACE303C4C771B46C8121FB6E46FA807E54787671DE13	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows	4	No
10	58B010F35B2616FACF99EB108732887844C1553D798B0475CD5EC78F34351C	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	3EDB46FC6E6A9CC12F599B78051C638E3E6A51453A0DFE8E3A3FFD6EA060DB7	PE32+ executable (GUI) x86-64, for MS Windows	0	Yes
14	8632A3DDE098D2C9CCCEBF4EFC8DEEBFAA9797EE9D20D9CA992E295A802E9	PE32+ executable (GUI) x86-64, for MS Windows	1	No
15	B9D1A099B496A9B34AE7399DF585477E00AADFB995297FB50F548DCFFAEA7BD	PE32 executable (GUI) Intel 80386, for MS Windows	11	No
16	879EBB0698C6F93D4E8E90B79E6A4B1256AF42543922613D6ED8644B8C2AA1	PE32 executable (native) Intel 80386, for MS Windows	20	No
17	A5072B34B8EFC127ED440355D21566152895CDFA1D57CA9F731BD368C3004AF	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows	4	No

Top 25 Yara Rules Matched Graph

Malware Analysis Dashboard

Dashboard
Real-Time Dashboard

FLAGGED FILES

- 65F31AE9563F9AAF782941FFA67BA...
- 955626A5C3A583353A135DD3737A0...
- D49BD707B4D52C21F1CE97961C965...
- 83DA562775023AF437CB18DFAF4C7...
- 1527FC7C5F13E4D2FC1BF8DA7D68C...
- 3ED84F6CFE6A9CC21F599B78051C6...
- E722DAB92F4B85A3FF8CA5158CB6...
- 2A225193A481E53920CF8351764F4...
- FBE2D7D678047B0BC43E78B09B36...

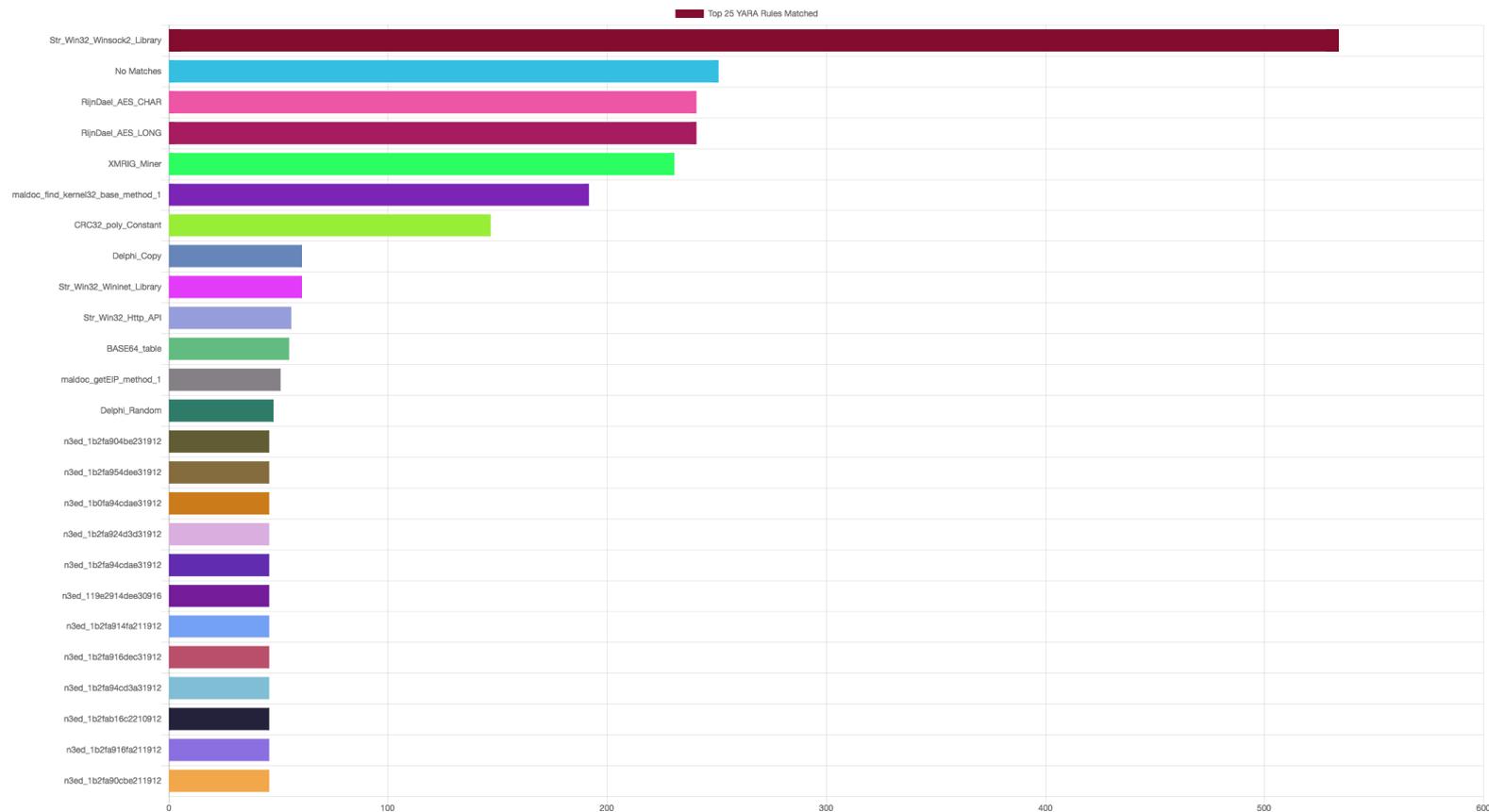
And 242 more files...

KNOWN MALWARE FILES

- 69CEFFE306948C50094B45D104431...
- 09CBE28B18E9DE87DE93E7E58EFAE...
- C6A13AFC5831096B0CCB54FBB2B3...
- 48678EC33D22C571774ACE303C4C7...
- 58B010F35B2616FACF99EEB10B7328...
- 69760CD6A5BF79558443BA6FCE64...
- 973DD088382AF4504E8F709E1BC605...
- 8632A3DDE098D2C9CCCEBF4EFC8D...
- B9D1A099B496A9B34AE739BDF585...

And 846 more files...

Top 25 Yara Rules Matched



File Info Page

Malware Analysis Dashboard

Dashboard

Real-Time Dashboard

FLAGGED FILES

- 65F31AE9563F9AAF782941FFA67BA...
- 955626A5C3A583353A135DD3737A0...
- D49BD707B4D52C21F1CE97961C965...
- 83DA562775023AF437CB18DAFA4C7...
- 1527FC7C5F13E4D2FC1BF87AD68C...
- 3ED84F6CFE6A9CC12F599B78051C6...
- E722DAB92F4B85A3FFF8CA5158C86...
- 2A225193A481E53920CF8351764F4...
- FBE2D7D678047B0BC43E78B09B36...

And 242 more files...

KNOWN MALWARE FILES

- 69CEFFE306948C50094B45D104431...
- 09CBE28B18E9DE87DE93E7E58FEAE...
- C6A13AFC583109680CCB54FBB2B3...
- 48678EC33D22C571774ACE303C4C7...
- 58B010F35B2616FACF99EEB1087328...
- 69760CD6A5B79558443BA6FCE64...
- 973D0B8382AF4504EBF709E1BC605...
- 8632A3DDE098D2C9CCCEBF4EFCBD...
- B9D1A099B496A9B34AE739BDF585...

And 846 more files...

PE Hash	3-N9K8gKRTeJ3HXKUQZDhBMgr8mmWkWoPWW2zjUjVUn:N7TENXPQdHfizWf/W2Pf2+
SHA256	13EE01EE8EA515C436D5110BE4612CEF3A4197343987303356DCEFFA37B01901
SHA1	F966381952994E7C21B6E6AC1D1A213EA315D895
MD5	7C3AA34A2A8AAFDB8695325D3A5436FB

Similar Malware

Show 10 entries

Search:

File Name	PE Hash
052676CE939DE75433B97C6A87086FD6D69C734B24B64A4C4579899A6CE3B0A	3-N9K8gKRTeJ3HXKVCTStg0BaoerhQmSWVRndYm8eckqu:N7TENXfetg0l0qnmwn
0C8CC948B56E18B4DEEC5E61951EA4FFBEC0CDF0200C54E63D7D6E26C0C9D	3-N9K8gKRTeJ3HXKvqRgnklHggm1QYcBgYfLVUL5RhShGn:N7TENXt6KwWdJYtIVHShGn
10F04B166222635BD2938A57A5FC6032B7029BD13F1AC3C8C26338566FC2F8	3-N9K8gKRTeJ3HXKUJwVtXXXtXbcVmo2JjdsaaQmhn:N7TENXPwbH1Gmo2/dsaazh
119D4046B4ADAB0224C190D0D99D33FAF02F4ABA18CE342F879274E4A2CC4D7	3-N9K8gKRTeJ3HXKU1VRehykP9CkPgWPS9XmmJ:N7TENXP5eh6ikPgWOXmmJ
1EAC00FD1299F38CF964B45482ACBB154E98F46D4B4D6705D6703ACF284808	3-N9K8gKRTeJ3HXKUgVjcadnZyQnfgczhrnRhtmb1J7kn:N7TENXPgbcavtnzh1b1kn
2075A75B5C991BF65E1A48FBFCE8D4E07A87552C367EFB0D643EFEC961683D1	3-N9K8gKRTeJ3HXKX4xbQtujjmMGvQx/bvFwgc0RWHL:N7TENXlxbQRmMCQtXfw2WhL
241813A80ABB18FCB0C9CEFAE0C292854898E06DFCC86663C30D2002EDB72	3-N9K8gKRTeJ3HXKXyefdqm2mgjRgVmwDedsEzHWLXunSzn:N7TENXBe1q/zRgzidsOU+v
2F0EA548E40A95C2809F5A4800D3ACBF0CD2680C4FEF39C8A35A2AA42309F9	3-N9K8gKRTeJ3HXKXjY7UvVjK0vzhXKajWz0kRXWEmn:N7TENXIM5ky4o3/n
3439D421368F3EBF63687DDA5A3948BCE563C1777B57948D12DB68C520E8F	3-N9K8gKRTeJ3HXKWPR5jnmShbcnmbSglUhrnXVgdjVn:N7TENXrjhtbcwJmRXVQVn
3661B212690D0FAEFC9F053F2060BD6F0BB3952CC9E8D5E8581B49036D696B2	3-N9K8gKRTeJ3HXKwWUXtqmS6KTvnFppm73nlUnphinx:N7TENXnwOTqZTVAJG

Showing 1 to 10 of 39 entries

Previous 1 2 3 4 Next

Yara Output

Show 10 entries

Search:

Rule	Namespace	Meta
maldoc_find_kernel32_base_method_1	rule13164	author: Didier Stevens (https://DidierStevens.com);
RijnDae_LAES_CHAR	rule13149	date: 2016-06; description: RijnDae AES (check2) [char]; author: .pusher_;
RijnDae_LAES_LONG	rule13149	date: 2016-06; description: RijnDae AES; author: .pusher_;
Str_Win32_Winsock2_Library	rule17	author: @adricnet; method: String match; description: Match Winsock 2 API library declaration;
XMRRIG_Miner	rule54	

Showing 1 to 5 of 5 entries

Previous 1 Next



Signature Generation Page

cuckoo Dashboard Recent Pending Search Submit Import

Automated Signatures

DNS 3

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?

?

?

?

?

?

?

?

?

?

