Using MISP for Bulk Surveillance of Malware

John Bambenek, Manager of Threat Systems
Fidelis Cybersecurity

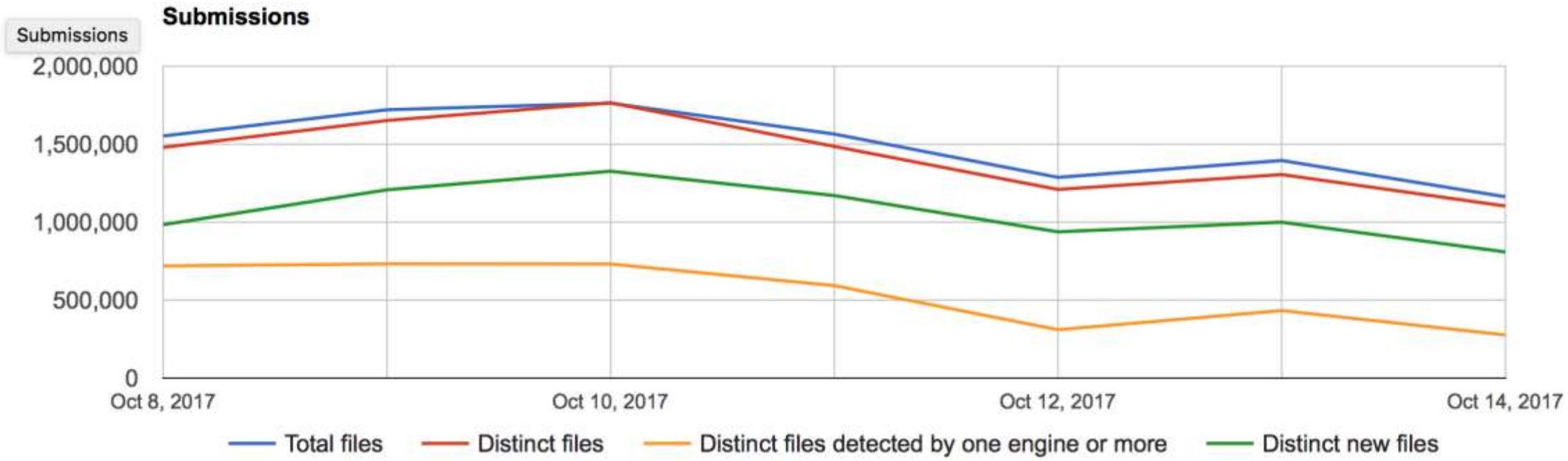
Fidelis™ Cybersecurity

Introduction

- Manager of Threat Systems with Fidelis Cybersecurity
- Handler with SANS Internet Storm Center
- Part-Time Faculty at University of Illinois in CS
- Provider of open-source intelligence feeds
- Run several takedown oriented groups and surveil threats

Shorter Version

The Problem Illustrated (from Virustotal)



The Reality

- There is a much smaller set of actual malware tools, many are used by multiple people.

- Problem: How to disambiguate the actual malware operator from the tool being used generally?

Malware Config Ripping

- Dynamic analysis is good, but bin may not run correctly and is resource intensive.
- Static analysis can be very fast… if you know how to pull the information out.
- Key is to automate such that you can do as much static analysis as possible, dynamic for much of the rest and RE only for the items where there is no other alternative.

Your Starter Kit

- Start with a feed of binaries, VT is fine or whatever you have. (Your own spam folders)
- Use Yara and/or AV names to preselect family.
- Run appropriate malware decoder
  - Put in whatever database makes sense to you.
  - Internally we use splunk, external sharing via MISP.
- All of this (Except the feed of malware*) is open-source and you can start doing this today.

What can you do with malware configs?

- Sinkholing for victim notification is a possibility.
- Mining the data for correlations.
- Mine historical database for indicators that didn’t seem important at the time but became important later.
- Share it with organizations all over the world.
  - Over 1200 users today.

Malware Configs

- Every malware has different configurable items.
- Not every configuration item is necessarily valuable for intelligence purposes. Some items may have default values.
- Free-form text fields provide interesting data that may be useful for correlation.
- Mutex can be useful for correlating binaries to the same actor.

Sample DarkComet Data

Key: CampaignID Value: Guest16
Key: Domains Value: 06059600929.ddns.net:1234
Key: FTPHost Value:
Key: FTPKeyLogs Value:
Key: FTPPassword Value:
Key: FTPPort Value:
Key: FTPRoot Value:
Key: FTPSize Value:
Key: FTPUserName Value:
Key: FireWallBypass Value: 0
Key: Gencode Value: 3yHVnheK6eDm
Key: Mutex Value: DC_MUTEX-W45NCJ6
Key: OfflineKeylogger Value: 1
Key: Password Value:
Key: Version Value: #KCMDDC51#

Sample njRat config

Key: Campaign ID Value: 1111111111111111111

Key: Domain Value: apolo47.ddns.net

Key: Install Dir Value: UserProfile

Key: Install Flag Value: False

Key: Install Name Value: svchost.exe

Key: Network Separator Value: |'|'|

Key: Port Value: 1177

Key: Registry Value Value: 5d5e3c1b562e3a75dc95740a35744ad0

Key: version Value: 0.6.4

All the fields…

ActivateKeylogger,ActiveXKey,ActiveXStartup,AddToRegistry,AntiKillProcess,BypassUAC,CONNECTION_TIME,Campaign,ChangeCreationDate,ClearAccessControl,ClearZoneIdentifier,ConnectDelay,CustomRegKey,CustomRegName,CustomRegValue,DELAY_CONNECT,DELAY_INSTALL,Date,DebugMsg,Domain,EnableDebugMode,EnableMessageBox,EncryptionKey,Error,ExeName,FTPDirectory,FTPHost,FTPInterval,FTPKeyLogs,FTPPassword,FTPPort,FTPRoot,FTPServer,FTPSize,FTPUser,FireWallBypass,FolderName,Gencode,GoogleChromePasswords,Group,HKCU,HKLM,HideFile,ID,INSTALL,INSTALL_TIME,Injection,InstallDir,InstallDirectory,InstallFileName,InstallFlag,InstallFolder,InstallMessageBox,InstallMessageTitle,InstallName,JAR_EXTENSION,JAR_FOLDER,JAR_NAME,JAR_REGISTRY,JRE_FOLDER,KeyloggerBackspace=Delete,KeyloggerEnableFTP,KillAVG2012-2013,MPort,MeltFile,MessageBoxButton,MessageBoxIcon,MsgBoxText,MsgBoxTitle,Mutex,NICKNAME,NetworkSeparator,OS,OfflineKeylogger,Origin,P2PSpread,PLUGIN_EXTENSION,PLUGIN_FOLDER,Password,Perms,Persistance,Port,PreventSystemSleep,PrimaryDNSServer,ProcessInjection,RECONNECTION_TIME,REGKeyHKCU,REGKeyHKLM,RegistryValue,RequestElevation,RestartDelay,RetryInterval,RunOnStartup,SECURITY_TIMES,ServerID,SetCriticalProcess,StartUpName,StartupPolicies,TI,TimeOut,USBSpread,UseCustomDNS,VBOX,VMWARE,Version,_raw,_time,adaware,ahnlab,baidu,bull,clam,comodo,compile_date,date_hour,date_mday,date_minute,date_month,date_second,date_wday,date_year,date_zone,escan,eventtype,fprot,fsecure,gdata,host,ikarus,immunet,imphash,index,k7,linecount,magic,malw,mc,mcshield,md5,nano,norman,norton,outpost,panda,product,proex,prohac,quickheal,rat_name,resys,run_date,section_,section_.BSS,section_.DATA,section_.IDATA,section_.ITEXT,section_.RDATA,section_.RELOC,section_.RSRC,section_.TEXT,section_.TLS,section_AKMBCZMH,section_BSS,section_CODE,section_DATA,section_ELTQHVWF,section_VDOJLYFM,section_YRKCHNMU,sha1,sha256,source,sourcetype,splunk_server,splunk_server_group,spybot,super,tag,tag::eventtype,taskmgr,times_submitted,timestamp,trend,uac,unique_sources,unthreat,vendor,vipre,windef,wire

Compare to my DGA feeds

```
############################################################
## Master Feed of known, active and non-sinkholed C&Cs indicators
##
## Feed generated at: 2017-10-16 09:16
##
## Feed Provided By: John Bambenek of Bambenek Consulting
## jcb@bambenekconsulting.com // http://bambenekconsulting.com
## Use of this feed is governed by the license here:
## http://osint.bambenekconsulting.com/license.txt
##
## For more information on this feed go to:
## http://osint.bambenekconsulting.com/manual/c2-masterlist.txt
##
## All times are in UTC
############################################################
aakamen.com,78.24.9.52,ns2.vshosting.cz|ns.aakamen.com|poski.vshosting.cz,78.24.9.52|89.235.0.2,Master
Indicator Feed for banjori non-sinkholed domains,http://osint.bambenekconsulting.com/manual/banjori.txt
aaskmen.com,45.33.9.234,ns1.mytrafficmanagement.com|ns2.mytrafficmanagement.com,45.79.11.218|45.79.4.188,Master
Indicator Feed for banjori non-sinkholed domains,http://osint.bambenekconsulting.com/manual/banjori.txt
aifamen.com,172.246.178.129,juming.dnsdun.com|juming.dnsdun.net,37.221.175.75|42.123.97.189|61.130.31.189|116.1
.237.119|122.228.80.248,Master Indicator Feed for banjori non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/banjori.txt
```

Example Config

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events
2017-09-20		External analysis	domain	jokeratef.hopto.org		Ports:5552		225418 225424 225425 225426 225427
2017-09-20		External analysis	comment	vt		Source		
2017-09-20		External analysis	sha1	68ae509911720b62453d41a13b257cc4a7a90c4d				
2017-09-20		External analysis	comment	Joker		Campaign ID		
2017-09-20		External analysis	comment	f34d5f2d4577ed6d9ceec516c1f5a744		Imphash		
2017-09-20		External analysis	comment	2017-09-18 09:20:21		Date Observed		
2017-09-20		External analysis	sha256	125c12832dc93a73fbdc91c65d1af33e4e70333366a5a6678386f92dfa90491d				
2017-09-20		External analysis	comment	{"InstallFlag": "False", "RegistryValue": "d3d6e45e7149ee25864bdd1e52b063aa", "Version": "0.7d", "InstallDir": "TEMP", "NetworkSeparator": "|'|'|", "Date": "2017-09-18 09:20:21", "sha256": "125c12832dc93a73fbdc91c65d1af33e4e70333366a5a6678386f92dfa90491d", "rat_name": "njRat", "imphash": "f34d5f2d4577ed6d9ceec516c1f5a744", "sha1": "68ae509911720b62453d41a13b257cc4a7a90c4d", "md5": "d026f0b4777eda352de779146ba4fdea", "Origin": "vt", "Domain": "jokeratef.hopto.org", "InstallName": "Google.exe", "magic": "PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly", "Campaign": "Joker", "section_.TEXT": "73b057bb1251ea9f1e1367de7d760fbc", "section_.RSRC": "0243c9a7f8755f2c2b18037cdad6cc91", "compile_date": "2017-09-08 20:41:07", "Port": "5552", "section_.RELOC": "3f1bf7cd85ab7f0d15fd62c31824bb5d"}		JSON config		

What can you do with this?

- If you receive a sample, check the configuration items against the balance of former samples to find a pattern of behavior.

- Hunt for interesting data and actors.

So let's say you get this malware…

9/2/15
5:27:06.000 AM


```
{ [-]
   DELAY_CONNECT: 1
   DELAY_INSTALL: 1
   Date: 2015-09-02 05:27:06
   Domain: nikresut015js.zapto.org
   INSTALL: true
   JAR_EXTENSION: fqLw1v
   JAR_FOLDER: wcnLIxbslsn
   JAR_NAME: Fresh_Bomb
   JAR_REGISTRY: COpaNxwcFs5
   JRE_FOLDER: UOStKe
   NICKNAME: August24rdBombing
   Origin: vt
   PLUGIN_EXTENSION: lykYQ
   PLUGIN_FOLDER: L0ZQqgmCGJ4
   Port: 2014
   SECURITY_TIMES: 5
   VBOX: true
   VMWARE: true
   magic: Zip archive data, at least v2.0 to extract
   md5: a1c9d4b1e522cfab79982917d7930cd6
   rat_name: JSocket
   run_date: 2015-09-03
   sha1: af9c898da3faa02e5d9ae25c5f9ced5ded7c603e
   sha256: be0f6903b3217c8df94c69dc0ea58ee1c07e92ab563bc4015f1a49a1dcf99acf
   times_submitted: 2
   unique_sources: 1
}
```

Sometimes interesting things come up

2004 Russian aircraft bombings

From Wikipedia, the free encyclopedia

The **Russian aircraft bombings of August 2004** were terrorist attacks on two domestic Russian passenger aircraft at around 23:00 on 24 August 2004. Both planes had flown out of Domodedovo International Airport in Moscow.

Contents [hide]

Background

- Now dead, but was Java-based multiplatform RAT, has a strong LatAm user base but at least one user may have Hezbollah ties.
- There is a strong “RATing” presence in Middle East attackers.
- There can be some laterally communication/knowledge sharing among “support” entities in terrorist groups.

Digging deeper

host nikresut015js.zapto.org

nikresut015js.zapto.org has address 50.7.199.164

30058 | 50.7.199.164 | 50.7.192.0/19 | US | arin | 2010-10-18 | FDCSERVERS - FDCservers.net,US

RRset results for nikresut015js.zapto.org/ANY

bailiwick zapto.org.

count 11

first seen 2015-09-30 00:24:21 -0000

last seen 2015-10-08 11:37:34 -0000

nikresut015js.zapto.org. A 50.7.199.164

Digging deeper

,1,1,2015-08-10 06:31:43,**nikresut015js.zapto.org**,true,fqLw1v,wcnLIxbslsn,Fresh_Bomb,COpaNxwcFs5,UOStKe,**AugustBombing**,vt,lykYQ,L0ZQqgmCGJ4,2014,5,true,true,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: Fresh_Bomb, INSTALL: true, JAR_EXTENSION: fqLw1v

,1,1,2015-07-02 09:52:30,**nikresut015js.zapto.org**,true,qSFai7,NfK3deVgu9o,1stJulyBombing,M1mDo7Mh4VF,gVJ0uD,JSocket,vt,SBVUC,aVCrh3IPVFP,2014,5,true,true,{PLUGIN_EXTENSION: SBVUC, JAR_NAME: **1stJulyBombing**, INSTALL: true, JAR_EXTENSION: qSFai7

,2015-09-03 17:55:59,**nikresut015js.zapto.org**,,vt,2014,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: **Fresh_Bomb**, INSTALL: true, JAR_EXTENSION: fqLw1v, times_submitted: 1, DELAY_CONNECT: 1, run_date: 2015-09-04, SECURITY_TIMES: 5, VBOX: true, Date: 2015-09-03 17:55:59, JRE_FOLDER: UOStKe, sha256: 422fc0d4c7286db9b16fe86fb420e255de96a88bc4b316af96060894cb548913, PLUGIN_FOLDER: L0ZQqgmCGJ4, unique_sources: 1, JAR_FOLDER: wcnLIxbslsn, JAR_REGISTRY: COpaNxwcFs5, NICKNAME: **Sep3rdtBombing**,

,2015-09-02 05:27:06,**nikresut015js.zapto.org**,,vt,2014,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: **Fresh_Bomb**, INSTALL: true, JAR_EXTENSION: fqLw1v, times_submitted: 2, DELAY_CONNECT: 1, run_date: 2015-09-03, SECURITY_TIMES: 5, VBOX: true, Date: 2015-09-02 05:27:06, JRE_FOLDER: UOStKe, sha256: be0f6903b3217c8df94c69dc0ea58ee1c07e92ab563bc4015f1a49a1dcf99acf, PLUGIN_FOLDER: L0ZQqgmCGJ4, unique_sources: 1, JAR_FOLDER: wcnLIxbslsn, JAR_REGISTRY: COpaNxwcFs5, NICKNAME: **August24rdBombing**

,2015-09-02 05:23:35,**nikresut015js.zapto.org**,,vt,2014,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: **Fresh_Bomb**, INSTALL: true, JAR_EXTENSION: fqLw1v, times_submitted: 1, DELAY_CONNECT: 1, run_date: 2015-09-03, SECURITY_TIMES: 5, VBOX: true, Date: 2015-09-02 05:23:35, JRE_FOLDER: UOStKe, sha256: a985f8803080c8308d6850de4be9a9f096f7733ca1f98c14074b65be1051447f, PLUGIN_FOLDER: L0ZQqgmCGJ4, unique_sources: 1, JAR_FOLDER: wcnLIxbslsn, JAR_REGISTRY: COpaNxwcFs5, NICKNAME: **August24rdBombing**

,2015-09-02 01:15:43,**nikresut015js.zapto.org**,,vt,2014,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: **Fresh_Bomb**, INSTALL: true, JAR_EXTENSION: fqLw1v, times_submitted: 1, DELAY_CONNECT: 1, run_date: 2015-09-03, SECURITY_TIMES: 5, VBOX: true, Date: 2015-09-02 01:15:43, JRE_FOLDER: UOStKe, sha256: 2723bfc312cb05b4f5d8460286e18c1834381a6d216e95ab22ef779ce5150ad2, PLUGIN_FOLDER: L0ZQqgmCGJ4, unique_sources: 1, JAR_FOLDER: wcnLIxbslsn, JAR_REGISTRY: COpaNxwcFs5, NICKNAME: **August24rdBombing**

,1,1,2015-07-02 09:52:30,**nikresut015js.zapto.org**,true,qSFai7,NfK3deVgu9o,1stJulyBombing,M1mDo7Mh4VF,gVJ0uD,JSocket,vt,SBVUC,aVCrh3IPVFP,2014,5,true,true,{PLUGIN_EXTENSION: SBVUC, JAR_NAME: **1stJulyBombing**, INSTALL: true, JAR_EXTENSION: qSFai7, times_submitted: 2, DELAY_CONNECT: 1, run_date: 2015-08-19, SECURITY_TIMES: 5, VBOX: true, Date: 2015-07-02 09:52:30, JRE_FOLDER: gVJ0uD, sha256: d448763f6f2b1e6fab1d00a2e87d6f88d6706853b6078b97d72518fb5c07afa3, PLUGIN_FOLDER: aVCrh3IPVFP, unique_sources: 2, JAR_FOLDER: NfK3deVgu9o, JAR_REGISTRY: M1mDo7Mh4VF, NICKNAME: JSocket

Dark Comet Campaign IDs

24597	Guest16	2747	Guest16_	755		406	All	337	Kurban
232	Hacked	193	HF	181	test	168	Col334	145	Solis
140	Hack	135	lol	129	Test	128	Guest	121	Victim
118	PC	118	Guest1	105	new-vict	105	1	102	kurban
99	Slave	96	No-IP	93	Vitima	85	User	70	HACKED
68	all	68	Server	68	Guest17	66	DOS	58	okay
55	hack	55	Kurbanla	53	228	50	apb	50	B--L--A-
49	Hacker	47	KURBAN	46	Arkade	44	DC	43	Opfer
42	Steam	41	Victime	41	HACK	40	server	40	hak
39	hacked	39	RAT	36	TestGues	36	DhjetoR	35	vitima
34	123	33	LOL	33	DarkCome	32	user	32	Trolld
32	Rat-1	31	MoyerSK	31	2	30	SPY	30	LucidsVi
29	trolled	29	teste	29	MSIL	28	BOT	27	WinUpdat
27	TEST	25	Rat	24	kurban01	24	Omegle	24	DeadPrez
24	Darkcome	23	Server1	23	Gerek po	23	CSGO	22	deneme
22	darkcome	22	Youtube	22	New	22	Minecraf	22	Bot
21	victime	21	test1	21	kurban1	21	Noob	21	M2BOB

Counter-intelligence

- Attacks know that we do this and actively throw mud in the water.
- Attacks could just as easily submit binaries to VT with fake information. Some indication people used VT to test detection.
- Just because a C2 is in a given country, attacker may be somewhere else.

Example

11/20/15
2:12:42.000 PM


```
{ [-]
   Campaign: All
   Date: 2015-11-20 14:12:42
   Domain: 8.8.8.8
   FireWallBypass: 0
   Gencode: qkttTB7XaVzk
   Mutex: DC_MUTEX-6R5BT6J
   OfflineKeylogger: 1
   Origin: vt
   Port: 1604
   Version: #KCMDDC51#
   compile_date: 2012-06-08 11:12:27
   imphash: 8033c11f8a2fdfc317e8655120579933
   magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
   md5: ffe6d90760977305d01a346a25995efe
   rat_name: DarkComet
   run_date: 2015-11-21
   section_.BSS: d41d8cd98f00b204e9800998ecf8427e
   section_.DATA: cb210a12278fc6b67accee22c52b9ad1
   section_.IDATA: 80655c280fee15e63402a8fc93041c3c
   section_.ITEXT: 7d01b8ffc56f096e211f89f0f28e5b49
   section_.RDATA: c1788dfeb92bbf0cff5aeaeaf1270ff8
   section_.RELOC: 590aac335a7094d529e15198df1c5920
   section_.RSRC: dea984d74cf7c8d9674bfe8db73d7cfc
   section_.TEXT: c8087ea6a249266ed1db0453229b76c2
   section_.TLS: d41d8cd98f00b204e9800998ecf8427e
   sha1: c5d171467fcbf07bc3be50c019b077b3792dd668
   sha256: 8f507788204bb8843c7a59ddf6ec2f29982587c5624fabb45e20c317c977c381
   times_submitted: 1
   unique_sources: 1
}
```


Show as raw text

Barncat Access

- For access, go to: https://www.fidelissecurity.com/resources/fidelis-barncat
  - Little less than 250k configs stored (150k or so queued to be added soon)
- Bring data local (Splunk, ES, whatever) for bulk data analysis.
- Go do good stuff with this data, put bad people in jail, protect consumers, etc...

Questions & Thank You!

John Bambenek / john.bambenek@fidelissecurity.com

Special thanks to Kevin Breen and many others for their research. Thanks to Tim Leedy and rest of my team for their effort on this.

Fidelis™ Cybersecurity