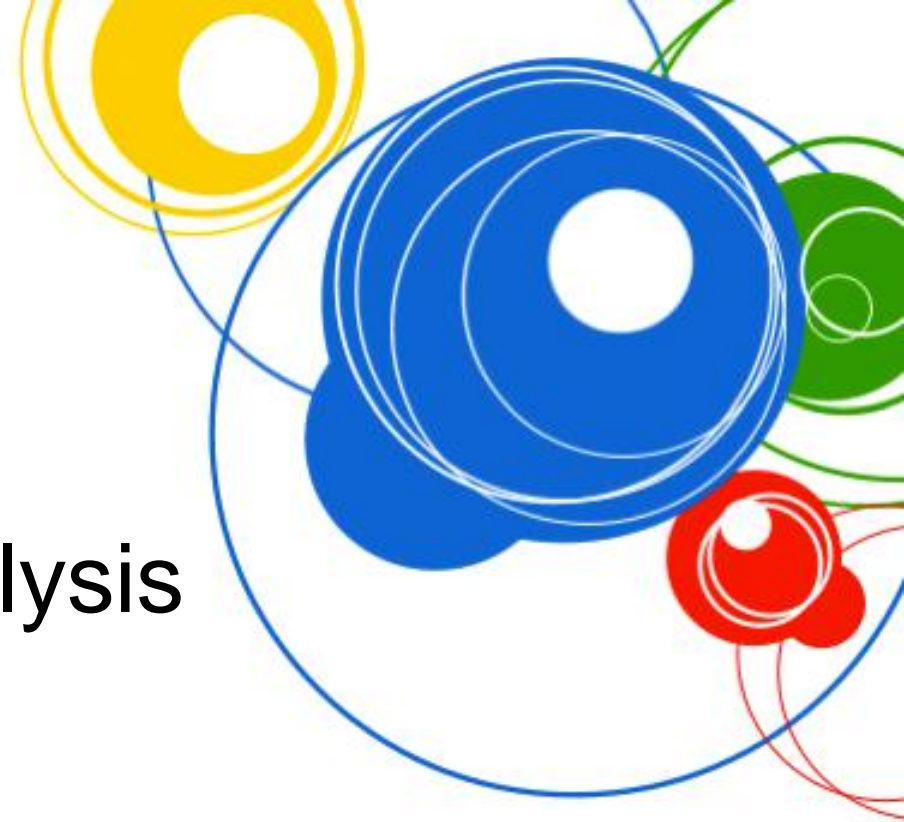


Taking Registry Analysis to the Next Level

Elizabeth Schweinsberg
After Pwn Technologist



Why I have Gathered you here Today

How can Registry Analysis help you find the badness on your systems?

- Overview of the favored Malware related Registry keys
- What keys are really being used in the wild?
- Which tools should you use for what?



Malware Related Keys

Run, RunOnce

- SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Services and Drivers

- SYSTEM\CurrentControlSet\Services
- Services Type is 0x10, 0x20, 0x100; Start is 2, 3, or 4 ONLY
- Drivers Type is 0x01 or 0x02; Start is 0 or 1 only??
- Services without “ObjectName” that is set to: LocalSystem, NT AUTHORITY\LocalService, or
- NT AUTHORITY\NetworkService
- Services starting under the Svchost process must have an entry in SOFTWARE\Microsoft\Windows NT\CurrentVersion\svchost



Malware Related Keys, cont.

Scheduled Tasks

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shared Task Scheduler
- SOFTWARE\Classes\CLSID\{GUID}

Browser Helper Objects

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

Winlogin and Subkeys

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin\Notify

How files are run

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts



Malware Related Keys, cont.

Application Initialization

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\ApplInit_DLLs

Actions that happen when cmd starts

- SOFTWARE\Microsoft\Command Processor\Auto Run

Boot Verification

- SYSTEM\CurrentControlSet\Control\BootVerificationProgram

Execute on Boot

- SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute



Where did you get these?

I read books and blogs and stuff

- Windows Forensic Analysis, 2nd Ed by Harlan Carvey
- Windows Registry Forensics by Harlan Carvey
- Footprints Under the Window by Franklin W. Dixon
- Windows Internals, 5th Ed by M Russinovich and D Solomon
- SANS DFIR blog
- Post Humorous Blog
- Windows IR blog



Then how do you know they're useful?

- Good question
 - Run keys are used all the time, but what about the others?
- Who would have a whole bunch of malware *and* have done some analysis about it?
 - AntiVirus companies, perhaps?
 - Repository of malware and technical analyses
<http://malware.lu>



Trawling the Symantec Site

Threat Explorer - Spywa x

www.symantec.com/security_response/threatexplorer/azlisting.jsp?azid=A

Overview Solutions Products Services Training Support Security Response Resources Community Store

Symantec.com > Enterprise > Security Response > Threat Explorer > A - Z Threats and Risks

Threat Explorer

The Threat Explorer is a comprehensive resource for daily, accurate and up-to-date information on the latest threats, risks and vulnerabilities.

Threat Landscape

Threat Explorer

Tools & Downloads

Removal Tools

Virus Definitions & Security Updates

Submit Virus Samples

Malware

Infected Systems

Resources

Blogs

White Paper Listing

Glossary

Overview Threats Risks Vulnerabilities A - Z Threats and Risks Search

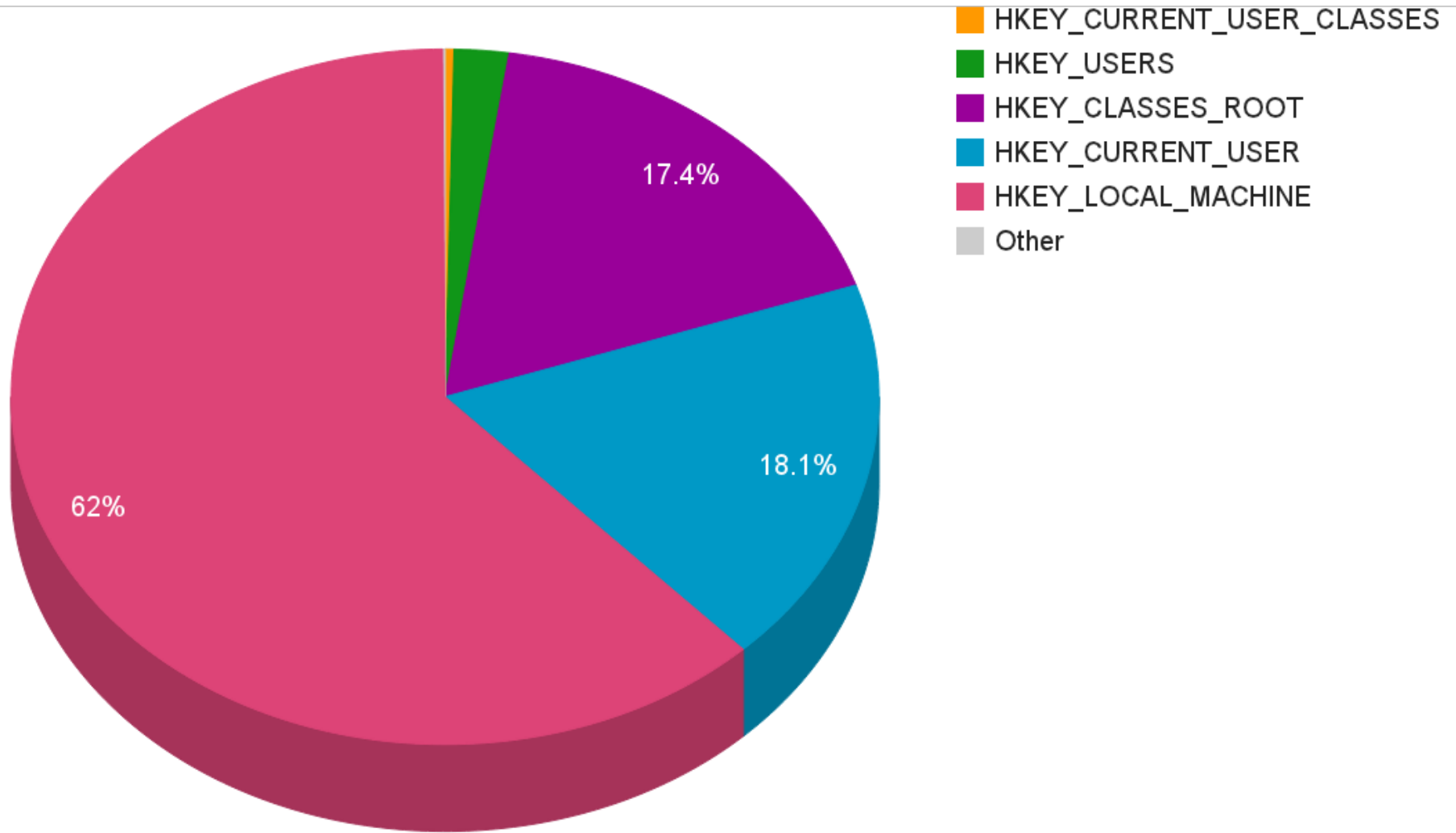
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0-9 Special Characters

Latest Threats & Risks

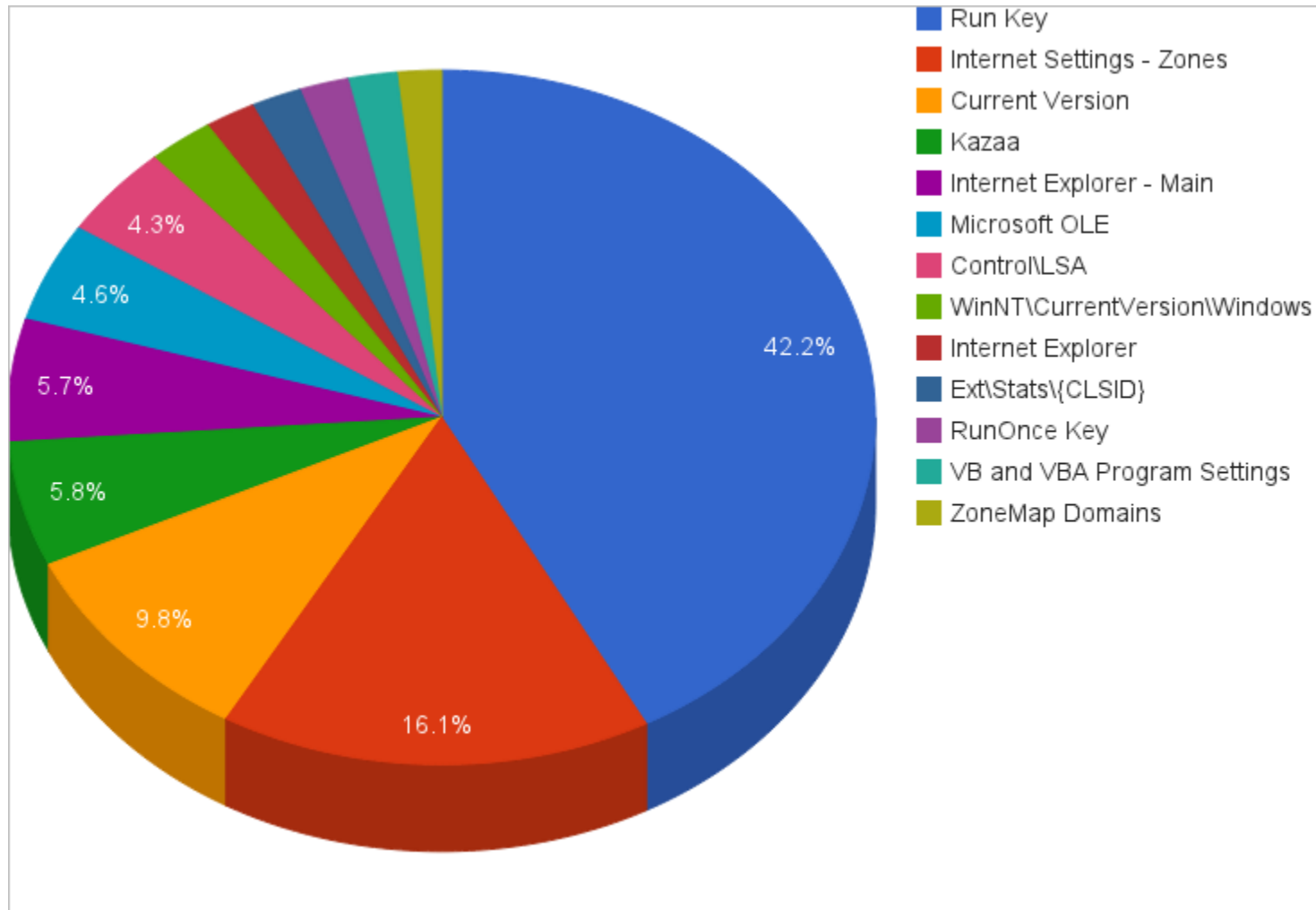
Symantec Security Response threat writeups (737)

Severity	Name	Type	Discovered
■ ■ ■ ■ ■	A and A	Virus	07/01/1993
■ ■ ■ ■ ■	A2K.Damcor	Worm	05/18/2004
■ ■ ■ ■ ■	A2M.Accessiv.A	Macro	
	A97M.Hamd.A	Macro	02/19/2002
	A97M.Loaded	Macro	02/19/2002
	A97M.Walla	Macro	02/19/2002
■ ■ ■ ■ ■	ABAP.Rivpas.A	Virus	04/14/2002
■ ■ ■ ■ ■	ABC	Virus	
■ ■ ■ ■ ■	Accept.3773	Virus	
■ ■ ■ ■ ■	ACTS.LFM.926	Virus	01/08/2002
■ ■ ■ ■ ■	ACTS.Spaceflash	Worm	07/18/2006
■ ■ ■ ■ ■	Ada	Virus	
■ ■ ■ ■ ■	Adolph	Virus	
	AdsAlert	Misleading Application	
	AdShortcuts	Potentially Unwanted App	
■ ■ ■ ■ ■	ADT.1765	Virus	04/03/2001
	AdvancedCleaner	Misleading Application	
	AdvancedXPFixer	Misleading Application	
	AdvParentalControl	Parental Control	
	Adware.123Search	Adware	

Trawling the Symantec Site



Trawling the Symantec Site - HKCU



Trawling the Symantec Site - HKCU

Not Malware Persistence per se...

Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden

Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt

Software\Microsoft\Windows\CurrentVersion\Explorer\
Advanced\ShowSuperHidden

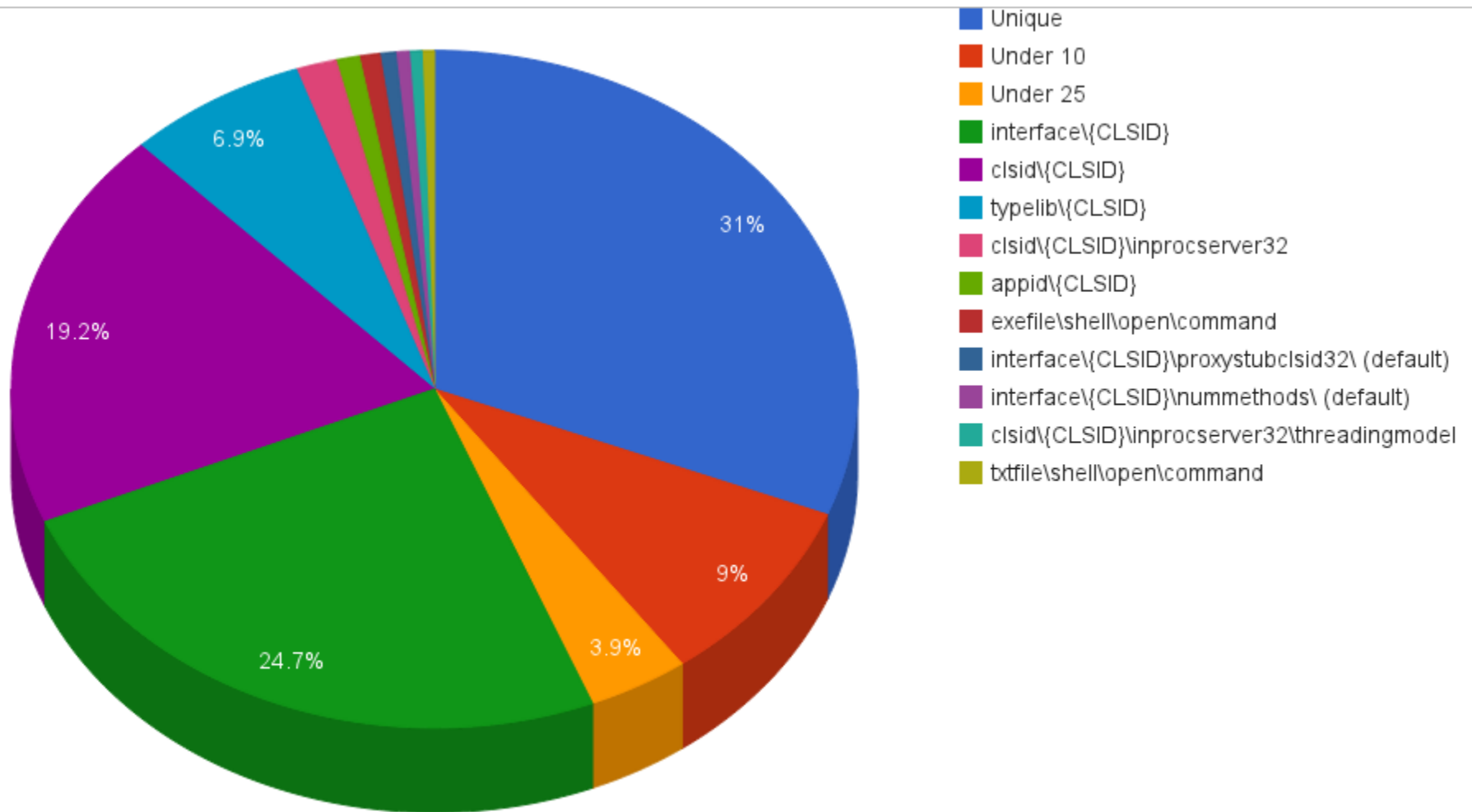
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFolderOptions

Software\Microsoft\Windows\CurrentVersion\Policies\
System\DisableRegistryTools

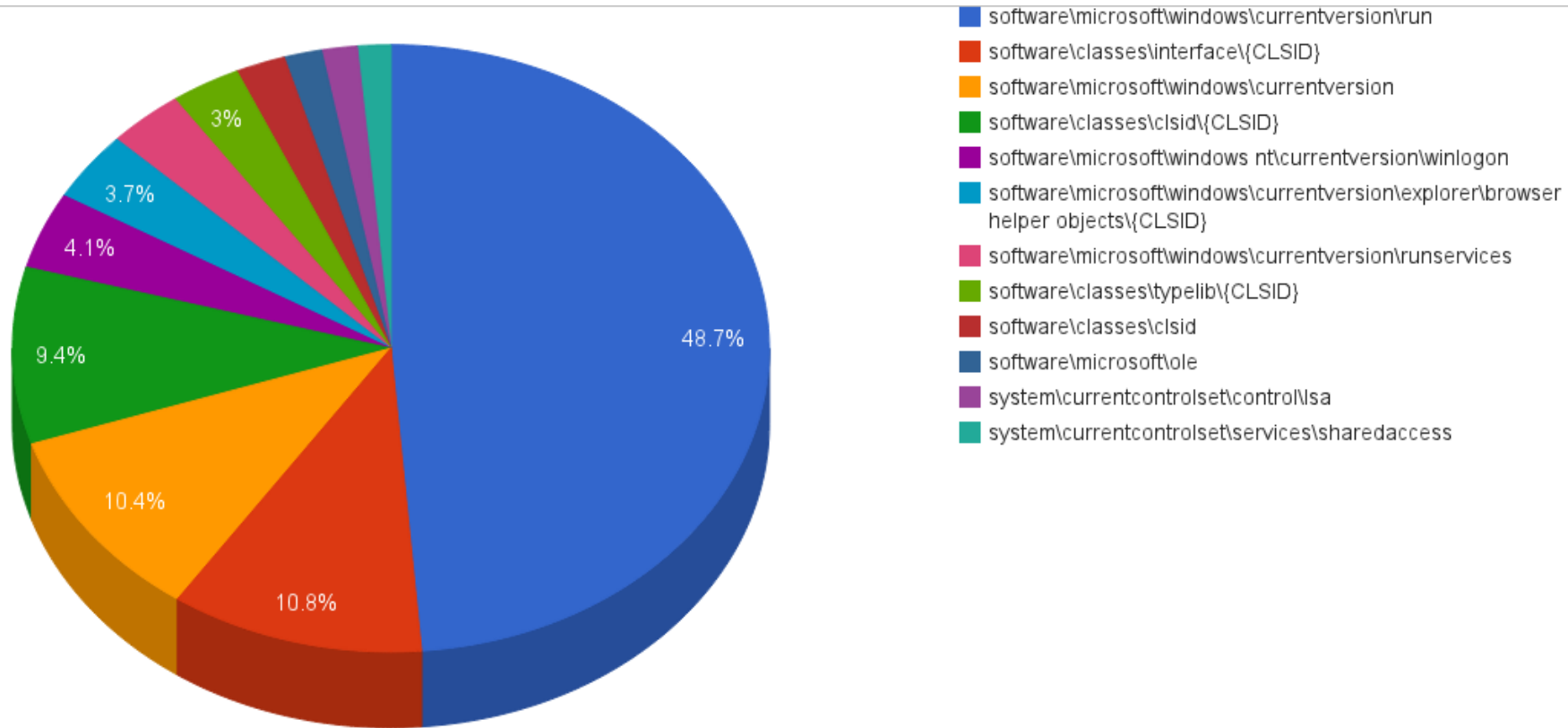
Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr



Trawling the Symantec Site - HKCR



Trawling the Symantec Site - HKLM



Trawling the Symantec Site - Compare

6360	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
283	SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
2521	SYSTEM\CurrentControlSet\Services
7	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shared Task Scheduler
365	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
423	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin
110	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin\Notify
5	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts
20	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\ApplInit_DLLs
3	SOFTWARE\Microsoft\Command Processor\Auto Run
0	SYSTEM\CurrentControlSet\Control\BootVerificationProgram
3	SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute



Keys to Keep

Keep	Downgrade	Add
<ul style="list-style-type: none">• Run• Services• WinLogon• Browser Helper Objects• AppInit_DLLs	<ul style="list-style-type: none">• BootVerification• Command Processor\Auto Run• BootExecute• Explorer\FileExts• Shared Task Scheduler	<ul style="list-style-type: none">• RunServices• RunOnce• Winlogin\Notify• VB and VBA Program Settings• Internet Settings\Connections• Internet Settings\Zones*• ZoneMap\Domains• Classes\{CLSID}\In ProcServer32



What do I even do with all these keys?

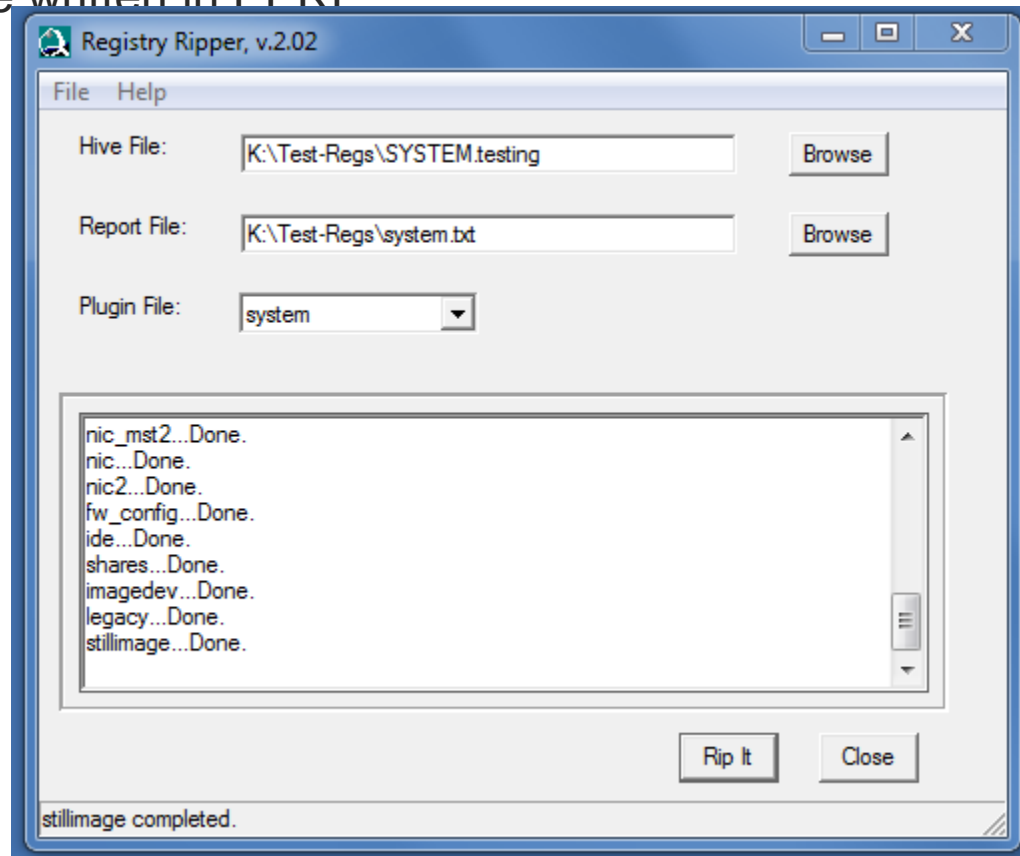


GRR Rapid Response
CBK BSIq Bezbovze

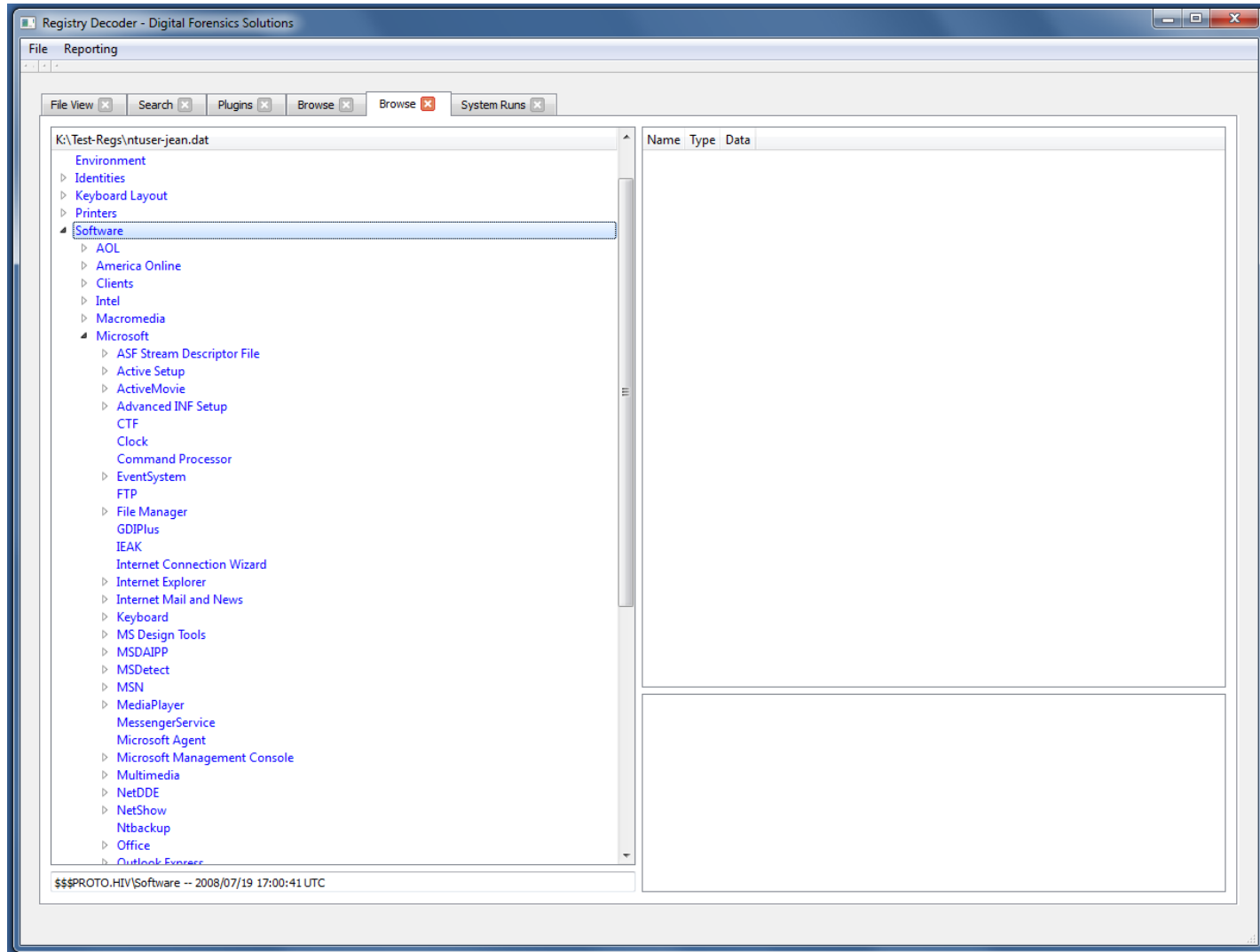


RegRipper

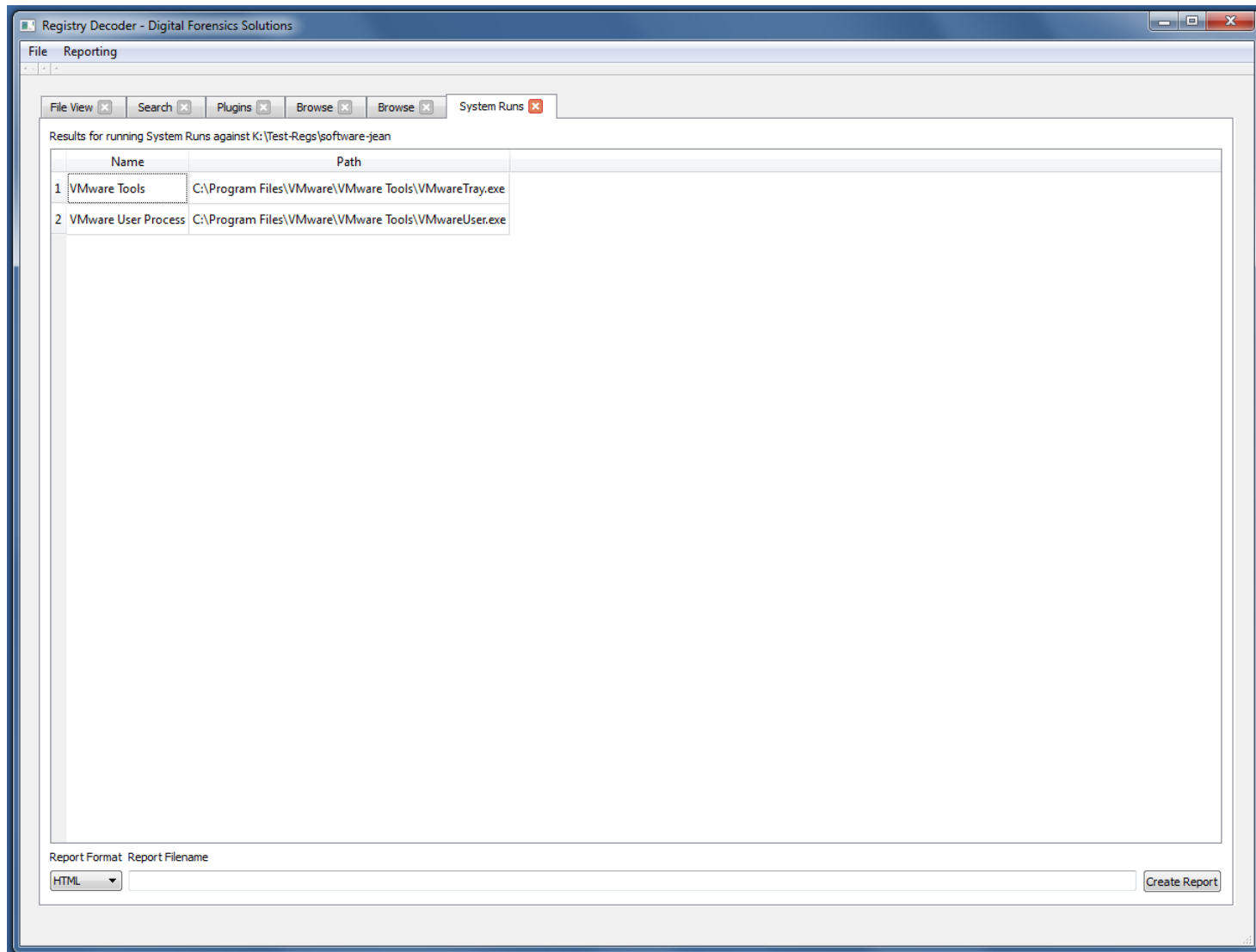
- PERL program with EXE
- Runs a set of plugins on a registry file and outputs the results into a textfile
- Plugins are written in PERL



Registry Decoder - Browsing



Registry Decoder - Plugins



Client ID	C.a0fdd4bb547cd31b
path	\\HKEY_LOCAL_MACHIN
pathtype	REGISTRY ▼
<button>Launch</button>	

Flow Information

Current Running Flows

GetFile

An efficient file transfer mechanism.

Returns to parent flow:

A jobs_pb2.Path.

Prototype: GetFile(path, pathtype)

Constructor.

This flow uses chunking and hashes to de-duplicate data and send it efficiently.

Args:

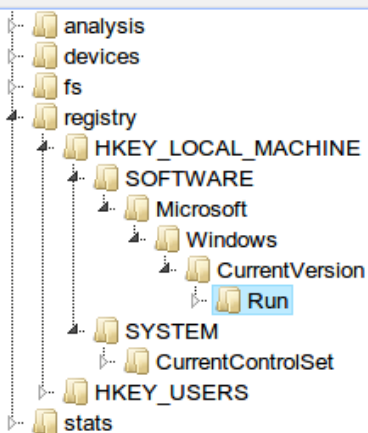
path: The directory path to list.

pathtype: Identifies requested path type. Enum from Path protobuf.

pathspec: This flow also accepts all the information in one pathspec. which is preferred over the path and pathtype definition

State	Description	Next States
Start	Get information about the file from the client.	Stat, ReadBuffer
Stat	Fix up the pathspec of the file.	End
ReadBuffer	Read the buffer and write to the file.	ReadBuffer

OPD - Incident Response - Forensics



Icon	Name	type	size	Age
	SunJavaUpdateSched	VFSFile	0	2012-06-18 20:23:54
	tvncontrol	VFSFile	0	2012-06-18 20:23:54

Stats

Download

TextView





HexView

aff4:/C.a0fdd4bb547cd31b/registry/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/SunJavaUpdateSched
@ 2012-06-18 20:23:54

Attribute	Value	Age
VFSFile, VFSAnalysisFile		
+ PATHSPEC	pathtype: REGISTRY path: "/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/SunJavaUpdateSched"	2012-06-18 20:23:54
+ STAT	aff4path st_mode st_size st_mtime registry_type pathspec registry_data	2012-06-18 20:23:54
	aff4:/C.a0fdd4bb547cd31b/registry/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/SunJavaUpdateSched ----- 60 2011-12-30 00:10:45 REG_SZ SunJavaUpdateSched "C:\Program Files\Java\Java Update\jusched.exe"	
	AFF4Image	
CHUNKSIZE	65536	2012-06-21 20:27:00
	AFF4Stream	
+ SIZE	0	2012-06-18 20:23:54
	AFF4Index, AFF4Object	
LABEL		2012-06-21 20:27:00
SUBJECT		2012-06-21 20:27:00
+ TYPE	VFSFile	2012-06-18 20:23:54

ORD RunKeyFlow

- analysis
 - RunKeys
 - LocalService
 - NetworkService
 - System
 - cyg_server
 - systemprofile
 - testing
 - devices
 - fs
 - registry
 - stats

Icon	Name	type	size	Age
	Run	RunKeyCollection	0	 2012-06-18 20:23:57
	RunOnce	RunKeyCollection	0	 2012-06-18 20:23:57

Stats

Download

TextView

HexView

aff4:/C.a0fdd4bb547cd31b/analysis/RunKeys/System/Run @ 2012-06-18 20:23:57

Attribute Value

Age

RunKeyCollection

RUNKEYS keyname: "/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/tvncontrol" 2012-06-18 20:23:57
filepath: "\"C:\\Program Files\\TightVNC\\tvnserver.exe\" -controlservice -slave" lastwritten: 1325203845
keyname:
"/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/SunJavaUpdateSched"
filepath: "\"C:\\Program Files\\Common Files\\Java\\Java Update\\jusched.exe\""" lastwritten: 1325203845

AFF4Index, AFF4Object

LABEL

2012-06-21 20:34:15

SUBJECT

2012-06-21 20:34:15

+ TYPE RunKeyCollection

2012-06-18 20:23:57



How do They Rate?

Compare and contrast the 3 tools over 2 samples:

- Testing VM with GRR, RegRipper and RegDecoder
 - Windows 7
 - Extracted the Registry files from the VM using GRR
 - LocalService and NetworkService Users point to the Default Users's NTUser.dat
- nps-2008-jean.E01 with RegRipper and RegDecoder
 - From the Digital Corpora images collection
 - Windows XP
 - Converted E01 file to raw, mounted as loopback and copied Registry files out
 - Could not get the raw image to boot as a VM, so could not test GRR



Testing VM

GRR	RegistryDecoder	RegRipper
Found 2 RunOnce keys: 1 in LocalService and 1 in NetworkService	RunOnce keys are listed under the Run key plugin	No plugin detects RunOnce keys
Found 1 Run keys: 1 in Local Service, 1 in NetworkService, and 2 in System	Found 4 Run keys: 2 in Default and 2 for System	Found 3 Run keys: 1 in Default and 2 in System
	2 BHO	3 BHO, but 2 were repeated
	NSTR in Services	NSTR in Services
	NSTR in WinLogon	NSTR in WinLogon



Jean NPS

GRR	RegistryDecoder	RegRipper
N/A	2 Run Keys for user Jean, 2 Run Keys for the system	2 Run Keys for user Jean, 2 Run Keys for the system
	NSTR in Services	NSTR in Services
	NSTR in WinLogon	NSTR in WinLogon
	1 BHO	1 BHO



Moving at Scale

GRR	Registry Decoder	RegRipper
<p>A work in progress...</p> <ul style="list-style-type: none">• Add Registry Flows to the initial interrogate flow so it is run every time a system is added• Use a Python script in the GRR console to iterate over all of the clients enrolled to both run the flow and collect results	<p>Not really built for scale</p>	<p>Once either the image is mounted or the registry files are extracted, write a script to run rip.exe across the files for all desired plugins</p> <pre>> rip.exe -r RegFile -p PluginModule</pre>



Tool Recap

GRR	Registry Decoder	RegRipper
<ul style="list-style-type: none">+ Registry Flows are quick+ Built to Scale- A work in progress... Best if you have a staff to keep it running	<ul style="list-style-type: none">+ Great UI+ Best for when you need to explore the registry and do targeted queries+ Written in Python+ Write your own plugins in Python- Cannot add a registry to a case once you've started	<ul style="list-style-type: none">+ Active Plugin Developer community+ Can be scripted to run across the registries you've extracted or mounted~ Write your own plugins in PERL



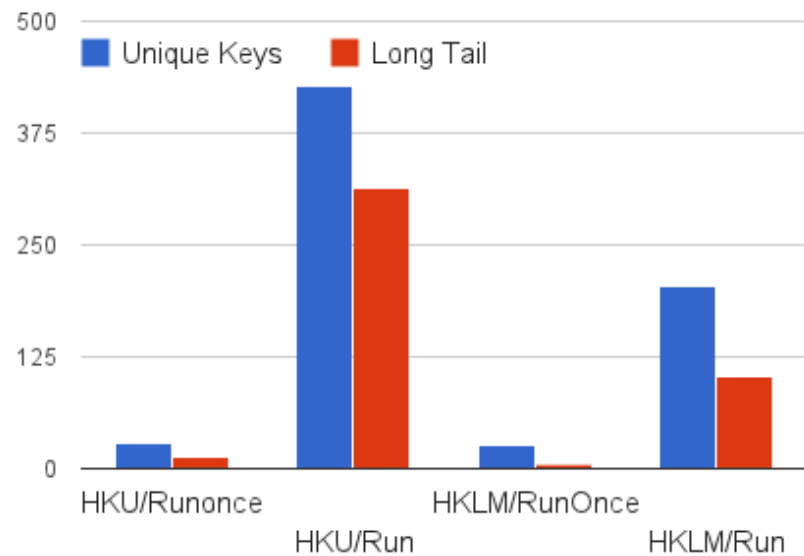
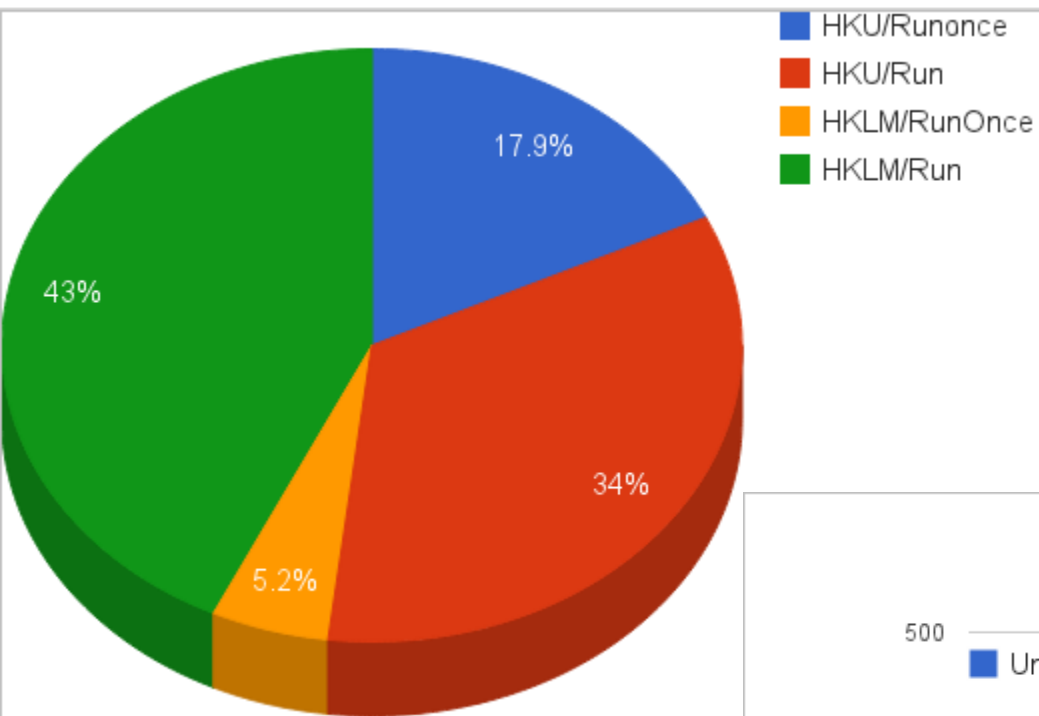
Analysis at Scale

Let's say some registry files fell off a truck...

- The long tail for Run keys is ~ 50% of the keys
- BUT the number of distinct values for Run keys is small
 - 86% of values had the same data (e.g. file path) when merely converting to all lowercase and removing usernames
 - Further improvements will be found with normalizing for version numbers



Analysis at Scale



Summary Judgement

How can Registry Analysis help you find the badness on your systems?

There are more keys to look at and research...
But a few to probably not worry about

If you aren't using RegRipper and Registry Decoder for your analysis -- start

Normalizing your Run keys will help you know when "it's probably fine"



Acknowledgments

NPS and Simson Garfinkle for the Digital Corpora project and images:

<http://digitalcorpora.org/>

The GRR Development Team!

<http://code.google.com/p/grr/>

Harlan Carvey for RegRipper

All the RegRipper plugin writers!

<http://regripper.wordpress.com/regripper/>

<http://code.google.com/p/winforensicaanalysis/downloads/list>

<http://code.google.com/p/regripperplugins/>

Digital Forensics Solutions for Registry Decoder

Andrew Case and Vico Marziale

<http://www.digitalforensicssolutions.com/registrydecoder/>



Google IR Road Show

BlackHat

July 25, 2012 in Las Vegas, NV

Morgan Marquis-Boire on CuteCats.exe and the Arab Spring

DFRWS

Sunday, August 5 2012 in Washington, DC

Dr. Michael Cohen on Memory Forensics with Volatility 3 hour Workshop

Open Source Digital Forensics Conference

October 3, 2012 in Chantilly, VA

Cory Altheide on ?? Does it even matter? It'll be hilarious **and** educational

Darren Bilby on GRR

Dr. Michael Cohen on Volatility

Joachim Metz on Volume Service Snapshot (VSS)

