Visual Malware Analysis with ProcDOT

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

Prerequisites/dependencies

Process Monitor[1]

GraphViz[2]

Windows or Linux operating system

As I write this I'm sitting in the relative darkness of the HolisticInfoSec lab listening to *Random Access Memories*, the new release from Daft Punk, and literally freaking out over what *Time* magazine's Jesse Dorris has glowingly referred to as a "sound for which the word epic seems to have been invented." Follow me as I step way out on a limb and borrow from Dorris' fine review to create a musical allegory for this month's topic, ProcDOT.[3] Dorris describes a "world in which the bounties of the past, present, and future have been Tumblr'd together into a stunning data blur."[4] I will attempt to make this connection with what ProcDOT's author, CERT.at's Christian Wojner, refers to as "an absolute must-have tool for everyone's lab." This is a righteous truth, dear reader; those malware analysts amongst you will feast on the scrumptious visual delight that ProcDOT creates.

We've not discussed visualization tactics in quite a while (March 2010[5]) but read on; the wait will be justified. ProcDOT, as described in Christian's March 2013 blog post, correlates Windows Sysinternals Process Monitor log files and PCAPs to an investigation-ready interactive graph that includes the animation of a malware infection evolution based on activity timelines.[6]

Christian gave me the full picture of his work creating ProcDOT to be shared with you here.

ProcDOT is the result of two ideas Christian had over the last few years. Initially he was thinking about the benefits of correlating Process Monitor logs with PCAP data to simple line charts with time and peaks as well as the ability to define tags for specific data situations. Sometime later, at the end of a malware investigation for a customer, he came to the point where he wanted to explain the characteristics of the underlying infection and depict the interaction of the malware's components as part of his final report. Christian found that a simple verbal description was both massively inefficient and insufficient at the same time (I confirm this shortcoming as well). Christian's thinking moved to the "big picture" in terms of a graph with nodes for the relevant objects as files, registry keys, etc., and edges for actions between them.

He then took the time to experiment with the Process Monitor logs he'd captured while trying to strip them down to the relevant content. This content he then manually converted to fit the input format of AT&T's Graphviz, chosen as a renderer for graphing. And there it was; a picture can tell a thousand words. It immediately became easy to understand all the aspects of the infection in one glance, even without any verbal explanation. That said, the manual activities to get to this result took about 50% of Christian's time during report generation and he had not yet included PCAP data at this point.

As the high potential of this approach proved itself obvious, Christian started to think about a tool that might take advantage of all this potential while bringing behavioral analysis a step further and making it accessible to non-malware analysts. Thus was born the ProcDOT project.

As ProcDOT is now close to its first official release, it is actually possible to automatically generate such a graph within seconds while also considering the information in an optionally supplied PCAP file correlating them with the Process Monitor logs. ProcDOT's infection evolution animation capabilities also eradicates the downside of older graphing techniques lacking the ability to effectively visualize the aspect of time.

Christian's road map (future think) for ProdDOT includes:

- Export capabilities for the graph
- Consider and provide much more information of PCAP data
- Time and context-dependent ranges of frames/events
- Customizable color themes
- Notes and tags
- Better GUI support of filters
- Session-related filters

[1] http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx.

[2] http://www.graphviz.org/Download..php.

[3] http://www.cert.at/downloads/summary/summary_en.html.

[4] Dorris, J. (2013, MAY 27). "Robots, rebooted." Elecro-pop duo daft punk's triumphant new record. *Time*, *181*(20), 60 – http://www.time.com/time/magazine/article/0,9171,2143561,00.html - ixzz2TvDgjDb6.

[5] http://holisticinfosec.org/toolsmith/docs/march2010.html.

[6] http://www.cert.at/services/blog/20130319171813-806_en.html.

This is a tremendous project and I look forward to its long life with ongoing support. As we run it through its paces I am quite certain you'll come to the same conclusion.

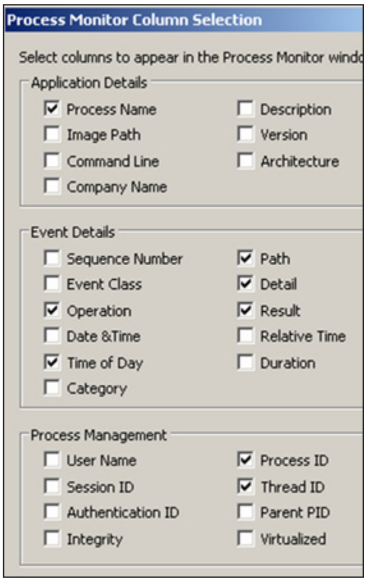
ProcDOT preparation

Christian has provided good documentation, including some easily avoided pain points that are worthy of repeating here. Process Monitor's configuration needs to be tuned to ensure ProcDOT compatibility.

In Process Monitor:

- Under *Options*, disable (uncheck) "Show Resolved Network Addresses"
- Via *Options* → Select *Columns*, adjust the displayed columns:
    - To not show the "Sequence Number" column
    - To show the "Thread ID" column

Figure 1 exemplifies the correct Process Monitor configuration.



Process Monitor Column Selection

Select columns to appear in the Process Monitor windo

Application Details

☑ Process Name ☐ Description
☐ Image Path ☐ Version
☐ Command Line ☐ Architecture
☐ Company Name

Event Details

☐ Sequence Number ☑ Path
☐ Event Class ☑ Detail
☑ Operation ☑ Result
☐ Date &Time ☐ Relative Time
☑ Time of Day ☐ Duration
☐ Category

Process Management

☐ User Name ☑ Process ID
☐ Session ID ☑ Thread ID
☐ Authentication ID ☐ Parent PID
☐ Integrity ☐ Virtualized

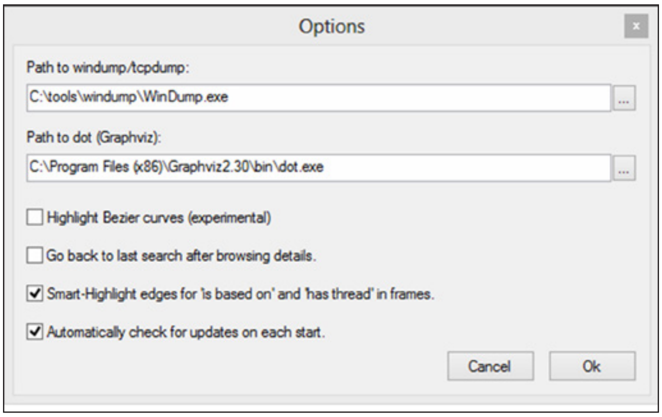
Figure 1 – Process Monitor configuration to support ProcDOT

ProcDOT also needs to know where its third-party tool dependencies are fulfilled.

In ProcDOT, under *Options*:

- Choose your Windump/Tcpdump executable as a fully qualified path
- Choose your Dot executable (dot.exe) as fully qualified path

Figure 2 shows my ProcDOT configuration as enabled on a 64-bit Windows 8 analysis workstation running the 64-bit version of ProcDOT. Keep in mind that the ProcDOT project releases a version that runs on Linux as well.



Options

Path to windump/tcpdump:
C:\tools\windump\WinDump.exe

Path to dot (Graphviz):
C:\Program Files (x86)\Graphviz2.30\bin\dot.exe

☐ Highlight Bezier curves (experimental)
☐ Go back to last search after browsing details.
☑ Smart-Highlight edges for 'is based on' and 'has thread' in frames.
☑ Automatically check for updates on each start.

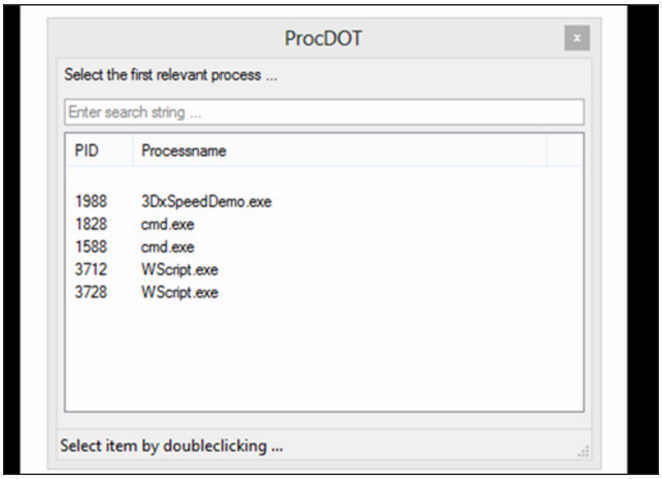
Figure 2 – ProcDOT tool path configuration

ProcDOT visualization

I worked with a couple of different samples to give you a sense of how useful ProcDOT can be during runtime analysis. I started with a well-detected Trojan dropper (Trojan/Win32.Qhost) from a threat-listed URL courtesy of Scumware.org, "just another free alternative for security and malware researchers," to trace interesting behavior when executing 3DxSpeedDemo.exe on a victim system. The MD5 for this sample is 20928ad520e86497ec44e1c18a9c152e, if you'd like to go get it for yourself. Alternatively, if you'd like to avoid playing with malware and just want the Process Monitor CSV and related PCAP, ping me via email or Twitter and I'll send them to you. I ran the malicious binaries on a 32-bit Windows XP SP3 virtual machine, capturing the related Process Monitor CSV log and the PCAP taken with Wireshark, then resetting to a clean snapshot for each subsequent analysis. You need to ensure that you save your default Process Monitor .PML file to .CSV which is easily done by selecting *Save*, choosing *All Events* and the CSV format. I copied the .PCAP and .CSV files from each run to my workstation and created visualizations for each.

Loading ProcDOT and readying it for a visualization run is simple. In the UI, select the appropriate CSV from *Procmon-CSV* field and PCAP from the *Windump-File* field. Note that the selection window for Windump-File defaults to Windump-TXT (*.txt); simply switch to Windump-PCAP (*.pcap) unless you actually generated text results. Check the no paths and compressed boxes, and hit *Refresh*.

This will generate an interactive graph, but you won't yet see results. You now must select the *Launcher*. ProcDOT will analyze the Process Monitor file; then ask you to select the first relevant process. This is typically the malicious executable (double-click it) you executed on your virtual machine or intentionally compromised system; again, 3DxSpeedDemo.exe for my first run, as seen in Figure 3.



ProcDOT

Select the first relevant process ...

Enter search string ...

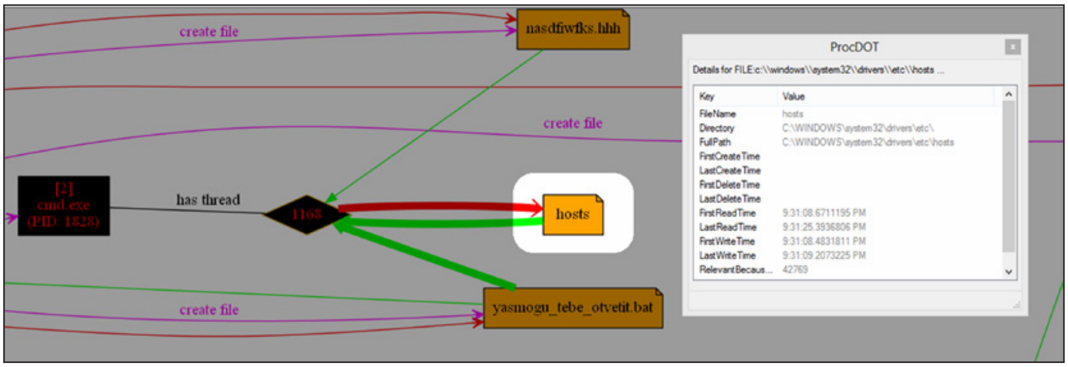
PID	Processname
1988	3DxSpeedDemo.exe
1828	cmd.exe
1588	cmd.exe
3712	WScript.exe
3728	WScript.exe

Select item by doubleclicking ...

Figure 3 – ProcDOT malicious process selection

Hit *Refresh* one more time and voila, your first visualization.

A few ProcDOT navigation tips:



ProcDOT

Details for FILE:c:\\windows\\system32\\drivers\\etc\\hosts ...

Key	Value
FileName	hosts
Directory	C:\WINDOWS\system32\drivers\etc\
FullPath	C:\WINDOWS\system32\drivers\etc\hosts
FirstCreateTime	
LastCreateTime	
FirstDeleteTime	
LastDeleteTime	
FirstReadTime	9:31:08.6711195 PM
LastReadTime	9:31:25.3936806 PM
FirstWriteTime	9:31:08.4831811 PM
LastWriteTime	9:31:09.2073225 PM
RelevantBecaus...	42769

Figure 4 – ProcDOT captures Win32.Qhost writing to the hosts file

- Hold CTRL and roll the scroll wheel on your mouse to zoom in and out.
- Hold your left mouse button while hovered over the graph to move it around in the UI.
- Double-click an entity to zoom in on it.
- Right-click an entity for details. Hit ESC to remove the highlighting.

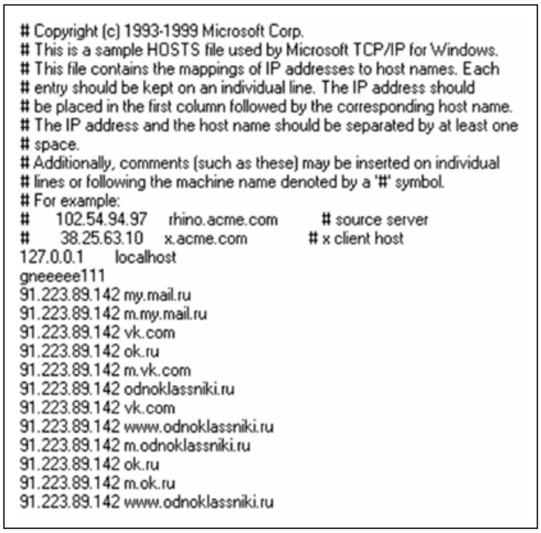
At the bottom of the UI if you click the film click, ProcDOT will move into playback mode and step through each process as it was captured. Remember our mention above of infection evolution animation capabilities that give you the ability to effectively visualize the aspect of time? Bingo.

Check out the legend under help (?) for the breakdown on the symbols used in graphing.

As I played back the Win32.Qhost infection, Frame 91 jumped out at me where thread 1168 of the cmd.exe process (PID 1828) wrote data to the hosts file as seen in Figure 4.

Oh snap! I love malware that does this. I jumped back to my malware VM, re-executed the malware, and captured the hosts file from C:\Windows\System32\Drivers\etc.

Figure 5 gives you an immediate sense of who the players are in this little vignette.



```
# Copyright (c) 1993-1999 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1       localhost
gneeeee111
91.223.89.142 my.mail.ru
91.223.89.142 m.my.mail.ru
91.223.89.142 vk.com
91.223.89.142 ok.ru
91.223.89.142 m.vk.com
91.223.89.142 odnoklassniki.ru
91.223.89.142 vk.com
91.223.89.142 www.odnoklassniki.ru
91.223.89.142 m.odnoklassniki.ru
91.223.89.142 ok.ru
91.223.89.142 m.ok.ru
91.223.89.142 www.odnoklassniki.ru
```

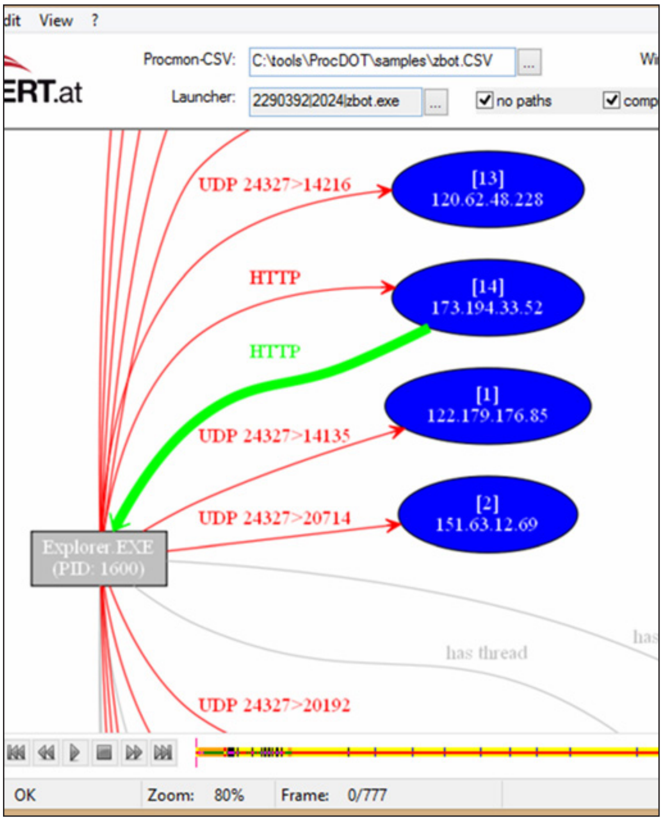
Figure 5 – You want me to login where?

The IP address 91.223.89.142 is indeed in the Russian Federation, but is not the appropriate A record for odnoklassniki.ru, or mail.ru, or vk.com, or ok.ru…you get the idea. I find it ironic that a seemingly Russian perpetrator is targeting Russian users as Eastern Bloc cybercriminals favor spreading their little bits of joy beyond their own borders. Just sayin'.

The Zbot sample I analyzed:

(MD5: 58050bde460533ba99d0f7d04eb2c80a)

made for great network behavior analysis with ProcDOT. I can't possibly capture all the glorious screen real estate here, but figure 6 should give you an idea of all the connections spawned by explorer.exe.



Procmon-CSV: C:\tools\ProcDOT\samples\zbot.CSV

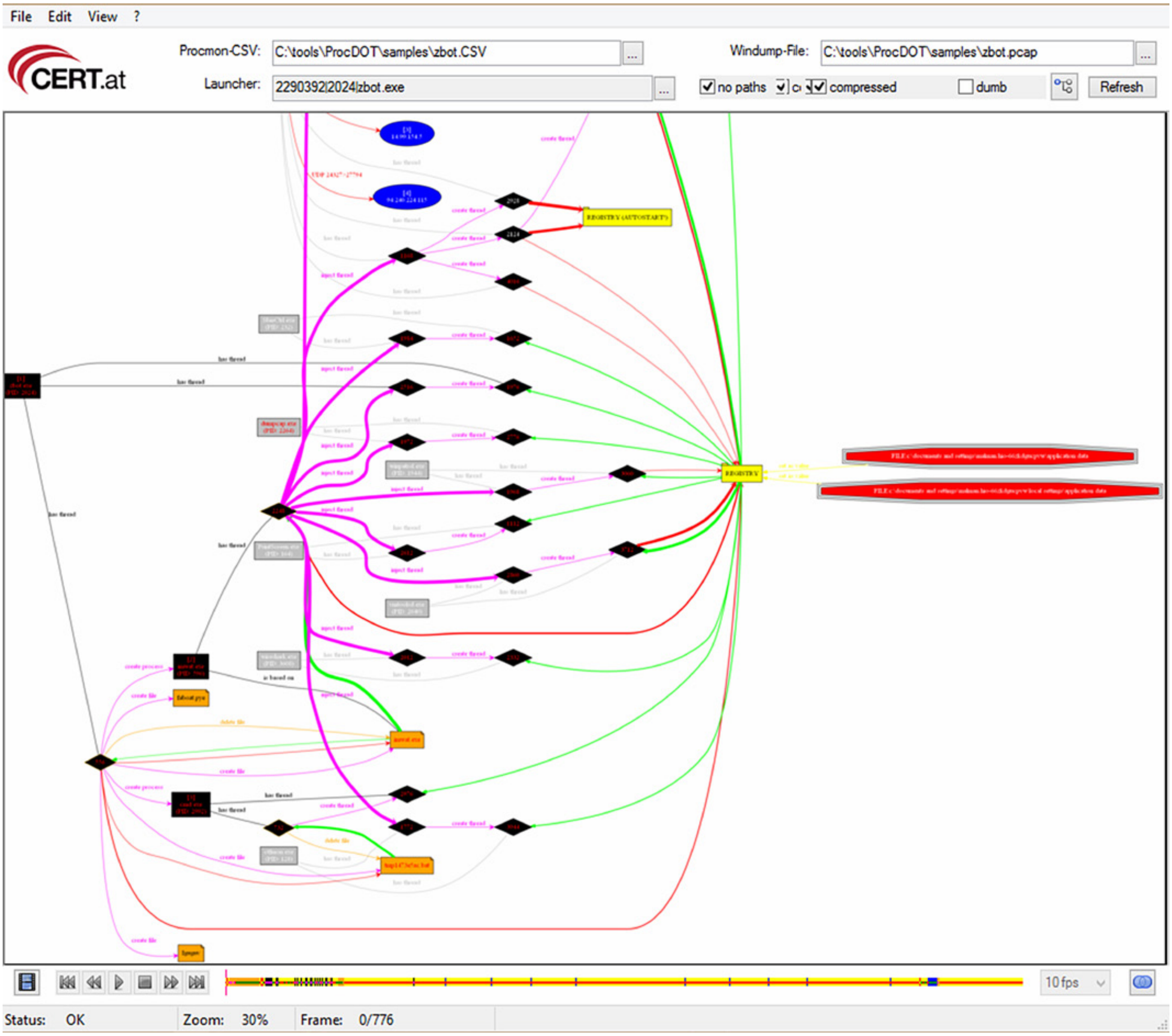
Launcher: 2290392|2024|zbot.exe

☑ no paths ☑ comp

OK Zoom: 80% Frame: 0/777

Figure 6 – ProcDOT network analysis

So many avenues to explore, so little time. Take the time; it's a rabbit hole you definitely want to go down. There's so much value in ProcDOT for malware analysts, incident responders, and forensicators. Paint a picture, cut to the quick, "the bounties of the past, present and future" await you in a "stunning



Procmon-CSV: C:\tools\ProcDOT\samples\zbot.CSV

Windump-File: C:\tools\ProcDOT\samples\zbot.pcap

Launcher: 2290392|2024|zbot.exe

☑ no paths ☑ ☑ compressed □ dumb

10 fps

Status: OK Zoom: 30% Frame: 0/776

Figure 7 – A stunning data blur…

data blur" created by ProcDOT. See figure 7 for enough proof to motivate you to explore on your own.

In conclusion

We've covered some truly kick@$$ tools already this year; Violent Python, SET, Redline, and Recon-ng put ProcDOT in some *major* company, but if I were able to vote for Toolsmith Tool of the Year in 2013, ProcDOT would be right at the top of my list. The current release is a still an RC; if you find any bugs let Christian know. The roadmap is solid so I am really looking forward to the stable releases soon to come. In particular, export capabilities for the graph will be a big step. Again, sample CSVs and PCAPs are available on demand.

Ping me via email if you have questions or suggestions for topic via russ at holisticinfosec dot org or hit me on Twitter @ holisticinfosec.

Cheers…until next month.

About the Author

Russ McRee manages the Security Analytics team (security incident management, penetration testing, monitoring) for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.