Threats & Indicators: A Security Intelligence Life Cycle

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

*borrowed directly from my parent team, thanks Elliot and Scott

Prerequisites

Microsoft .NET Framework, Version 3.5 or higher for IOCe

Python 2.7 interpreter for OpenIOC to STIX

I've been feeling as if it's time to freshen things up a bit with *toolsmith* and occasionally offer a slightly different approach to our time-tested process. Rather than always focusing on a single tool each month (fear not, we still will), I thought it might be equally compelling, perhaps more, if I were to offer you an end-to-end scenario wherein we utilize more than one tool to solve a problem. A recent series I wrote for the SANS Internet Storm Center Diary—a three-part effort called "Keeping the RATs Out"[1] —proved, I believe, how useful this can be.

I receive and review an endless stream of threat intelligence from a variety of sources. What gets tricky is recognizing what might be useful and relevant to your organizations and constituencies. To that end I'll take one piece of recently received intel and work it through an entire life cycle. This intel came in the form of an email advisory via the Cyber Intelligence Network (CIN) and needs to remain unattributed. The details, to be discussed below, included malicious email information, hyperlinks, redirects, URL shorteners, ZIP archives, malware, command and control server (C2) IPs and domain names, as well as additional destination IPs and malicious files. That's a lot of information, but sharing it in standards-based, uniform formats has never been easier. Herein is the crux of our focus for this month. We'll use Mandiant's IOCe[2] to create an initial OpenIOC[3] definition, Mitre's OpenIOC to STIX,[4] a Python utility to convert OpenIOC to STIX, STIXviz[5] to visualize STIX results, and STIX to HTML,[6] an XSLT stylesheet that transforms STIX XML documents into human-readable HTML. Sounds like a lot, but you'll be pleasantly surprised how bang-bang the process really is. IOC represents *Indicators of Compromise* (in case you just finally just turned off your vendor buzzword mute button) and STIX stands for *Structured Threat Information eXpression*. STIX, per Mitre, is a "collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information." It's well worth reading the STIX use cases.[7] You may recall that Microsoft recently revealed the Interflow[8] project, which incorporates STIX, TAXII (Trusted Automated eXchange of Indicator Information), and CybOX (Cyber Observable eXpression standards) to provide "an automated machine-readable feed of threat and security information that can be shared across industries and community groups in near real time." Interflow is still in private preview, but STIX, OpenIOC, and all these tools are freely and immediately available to help you exchange threat intelligence.

The intel

As received from the undisclosed source via CIN, following is the aggregated threat telemetry:

- **Email Subject**: Corporate eFax message
- **Email "Sender"**: eFax Corporate <message@inbound.efax.com>
- **Malicious Email Link**: hxxp://u932475.sendgrid.org/wf/click?upn=<redacted, and no longer active or useful>
- **Redirects to**: hxxps://goo.gl/A4Q0QI (still active as this is written)
- **Expands to**: hxxps://www.cubbyusercontent.com/pl/Fax_001_992819_12919.zip/_3f86d70bed3843eda9497a5d36ed8590
- **Drops**: Temp1_Fax_001_992819_12919.zip
- **Contains**: Fax_001_992819_12919.scr
  - Malware is CryptoWall variant[9]:
    - MD5: 668ddc3b7f041852cefb688b6f952882
    - SHA1: 2bbab6731508800f3c19142571666f-8cea382f90
- **C2**:
  - hxxp://sanshu.mamgou.net/wp-content/themes/xs/iiaoeoix7c
  - hxxp://pannanawydaniu.com.pl/wp-content/themes/marriage/w8z0ana

1 http://aka.ms/RATsPart1; http://aka.ms/RATsPart2; http://aka.ms/RATsPart3.
2 http://www.mandiant.com/resources/download/ioc-editor/.
3 http://www.openioc.org/.
4 https://github.com/STIXProject/openioc-to-stix.
5 https://github.com/STIXProject/stix-viz.
6 https://github.com/STIXProject/stix-to-html.
7 http://stix.mitre.org/language/usecases.html.
8 http://www.microsoft.com/interflow.
9 https://www.virustotal.com/en/file/ef953a03f9d7a43ddfc860cecb79df91634ced2186f38e59515dd37d235d9705/analysis/.

  - hxxp://stephanelouis.com/wp-content/themes/gather/9a6ct47znvpi
  - hxxp://delices-au-chateau.fr/wp-content/themes/squash/9b0t1f0koe8
  - hxxp://amedsehri.com/wp-content/themes/exiportal/dh5x3a1815j
  - hxxp://ciltbakim.org/wp-content/themes/baywomen/0ebac31z
  - hxxp://papillon-northwan.com/wp-content/themes/dog02_l/3sab5
  - hxxp://gsxf119.com/wp-content/themes/live-color/k7eh5zug5vq7
- Destination IPs and related domains
  - 212.112.245.170
    - hxxps://www.abyrgvph4qwipb5w2zb.net
  - 86.59.21.38
    - hxxps://www.kxglgw6f2fg2g.net
    - hxxps://www.fp5jrlfn5d6s.net
    - hxxps://www.3w64ehhmrz.net
  - 213.186.33.17
    - hxxp://delices-au-chateau.fr/wp-content/themes/squash/9b0t1f0koe8
    - hxxp://nitrofirex.com/wp-content/uploads/2014/07/tor2800.tar
      - tor2800.tar[10]
        - MD5: 14bbdcd-889ec963d7468d26d6d9c1948
        - SHA1: 39d3bc26b8b6f681c-c41304166f76f01eee5763b

Additional analysis in my malware sandbox yielded the following information:

- Each time the .scr is executed, it spawns a randomly named portable executable, negating the value of using said name as an indicator.
  - That said, the randomly generated PE spawns an additional PE file, consistently named dttey.exe
  - Dttey.exe deletes the randomly named PE that spawned it, and itself spawns vsspg.exe
  - There is extensive registry modification by all of the above mentioned PEs, some of which we can use for IOCs
  - Randomly named PE is Ransom:Win32/Crowti[11] (CryptoWall)
    - Malware encrypts files on victim PC using a public key.
    - The files can be decrypted with a private key stored in a remote server.
    - Recovery of files is via a personal link that directs you to a Tor webpage asking for payment using BitCoin. The above mentioned IP, 86.59.21.38, is a TOR node. Netresec's Erik Hjelmvik (CapLoader, Networkminer) covered this node as part of a deeper analysis[12] well worth your reading.
  - Review the Anubis analysis[13] as supplemental information

Figure 1 – CryptoWall decryption "service"

A compromised victim would be treated to a "service" to decrypt their files as seen in figure 1. These spectacular @$$h@ t$ even offer a very detailed instruction file that pops up, including an FAQ. What I wouldn't do to these people…

This is more than enough information with which to build a very useful and portable profile, starting with Mandiant's OpenIOC and IOCe.

OpenIOC and IOCe

Per Mandiant, who created OpenIOC, it is "an extensible XML schema that enables you to describe the technical characteristics that identify a known threat" and allows for "quickly detecting, responding, and containing targeted attacks." Mandiant IOCe allows you to edit and create OpenIOC definitions with ease. Once downloaded and installed, IOCe 2.2.0 opens to a fairly simple, rudimentary UI and workspace. Give the user guide installed with IOCe a read; you'll see a shortcut for it in your start menu. At first run you'll need to establish a directory for your IOCs. Go grab the examples from the OpenIOC website as well (under Resources) and drop them in your newly created directory; they serve as good reference material as you begin to build your own.

I always include a description of the parent evil for which I'm populating indicators and give the .ioc a relevant name for the UI list. Recognize that the actual .ioc filename will be the GUID that IOCe generates for it. IOCe utilizes simple AND OR operators for its logic. Basic IOCs can be a collection of OR items; if you use the AND operator all connected elements must be true or the logic fails.

Given the data from the intel provided above, each entity would be added to the IOC definition via the *Add: AND OR Item* menu. *The Item* is an expending dropdown menu divided into multiple IOC families such as Email, FileItem, PortItem, and RegistryItem, all of which we'll use given the data provided. You'll find the Most Commonly Used Indica-

10 https://www.virustotal.com/en/file/5c9062595ce8a1dedd409220ea8e4b9fb3cfb84e58dccff05465c03809be6a23/analysis/.

11 http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Ransom:Win32/Crowti&ThreatID=-2147279730 - tab=2.

12 http://www.netresec.com/?page=Blog&month=2013-04&post=Detecting-TOR-Communication-in-Network-Traffic.

13 https://anubis.iseclab.org/?action=result&task_id=1aa588d442308663459e4186ef9f29dab.

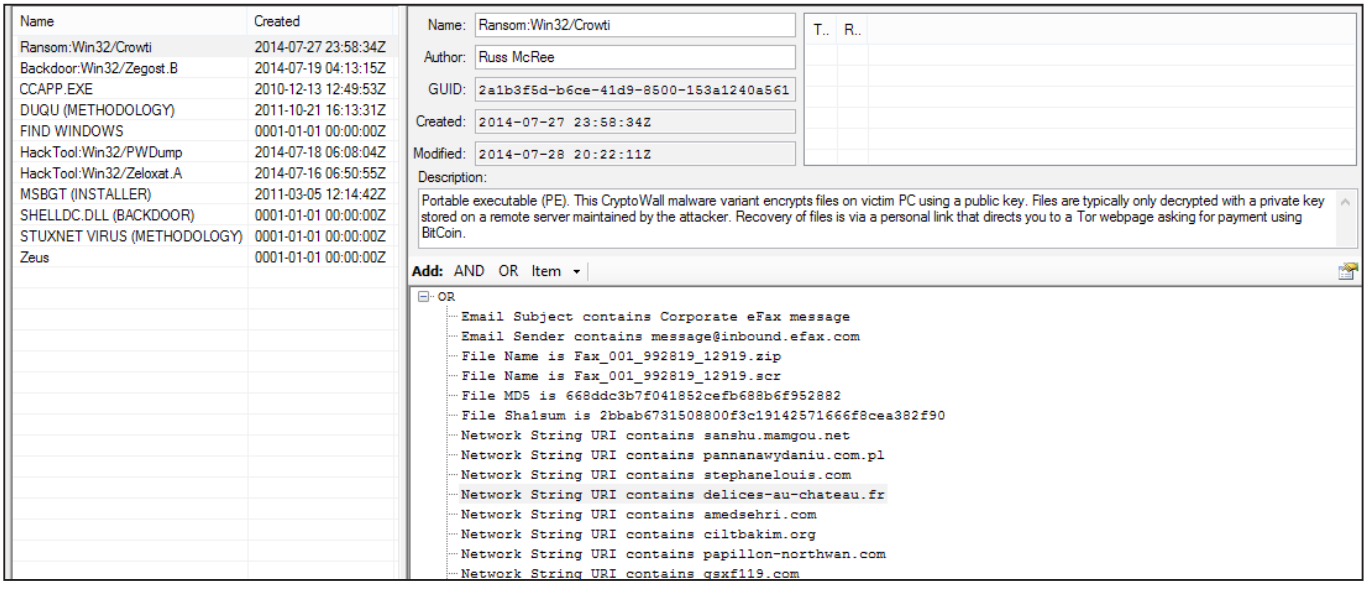


Figure 2 – IOC definition for CryptoWall variant created with IOCe

tor Terms[14] section of OpenIOC.org very useful to more easily search specific entries. Also keep in mind that both Mandiant Redline and Intelligent Response utilize and generate IOC definitions.

After generating all the related entries the resulting definition appears as seen in figure 2.

You can use this IOC definition with your Mandiant tools that consume it, or open it in IOCe to extract the indicators you may wish to add detection for via other tooling. This IOC, Ransom:Win32/Crowti (2a1b3f5d-b6ce-41d9-8500-153a1240a561.ioc[15]) can be found on my website if you'd like to use it try these tools out.

We now have the opportunity to convert this .ioc file into STIX.

OpenIOC to STIX

OpenIOC to STIX conversion is easily accomplished with Mitre's *openioc_to_stix.py* script, which is simply an OpenIOC XML to STIX XML converter.

One note, as I was writing this I was having trouble with the two email entities we added to the IOC definition; *openioc_to_stix.py* crashed until I pulled those entries.

You'll need a system with a Python 2.7 interpreter available and Pip installed. You'll need to then use Pip to install the Python STIX and Cybox library dependencies[16]:

```
pip install stix
pip install cybox
```

Then download and unpack the openioc-to-stix ZIP package or use the Git clone option. Once you have dependencies met and the scripts in place, you need only run `python openioc_to_stix.py -i <OpenIOC XML file> -o <STIX XML file>`. To convert the IOC definition I created above, I simply ran `python openioc_to_stix.py -i 2a1b3f5d-b6ce-41d9-8500-153a1240a561.ioc -o CryptoWallVariant.xml` after commenting out the email-indicator-related markup; I've also hosted this file[17] for your use.

STIXViz

STIXViz is really easy to install and run. Just download and unpack the package appropriate for your system then execute (StixViz.exe for Windows).

STIXViz is best exemplified with a more complex STIX file such as a Cyber Information Sharing and Collaboration Program (CISCP) Consolidated Indicators as collected by the IT-ISAC (Information Sharing and Analysis Center) and sourced from US-CERT Current Activity data. Note that you need to be an IT-ISAC member for access to these. STIXViz is written by Mitre's Abigail Gertner and Susan Lubar and, for those of you who share my fondness for visualization, will represent a wonderful vehicle to do so with threat data. STIXViz includes Graph, Tree, and Timeline views. The Tree view is likely to be deprecated but the Graph View includes linking and relationship labeling (think Maltego), while the Timeline View "shows timestamped STIX data, such as incidents and their associated events, in a zoomable, scrollable display" as noted in release notes. Simply open STIX and select the STIX XML you wish to visualize from your file system via the *Choose Files* button. Once opened, you can select indicators of interest. I selected exfiltration indicators as seen in figure 3.

You will definitely enjoy playing with STIXViz and manipulating the view options as you can pin, freeze, and group until you've perfected that perfect report snapshot.

Speaking of that report, want to turn threat data into nicely managed HTML? You can *Show HTML* in STIXViz or use the STIX XML to HTML transform.

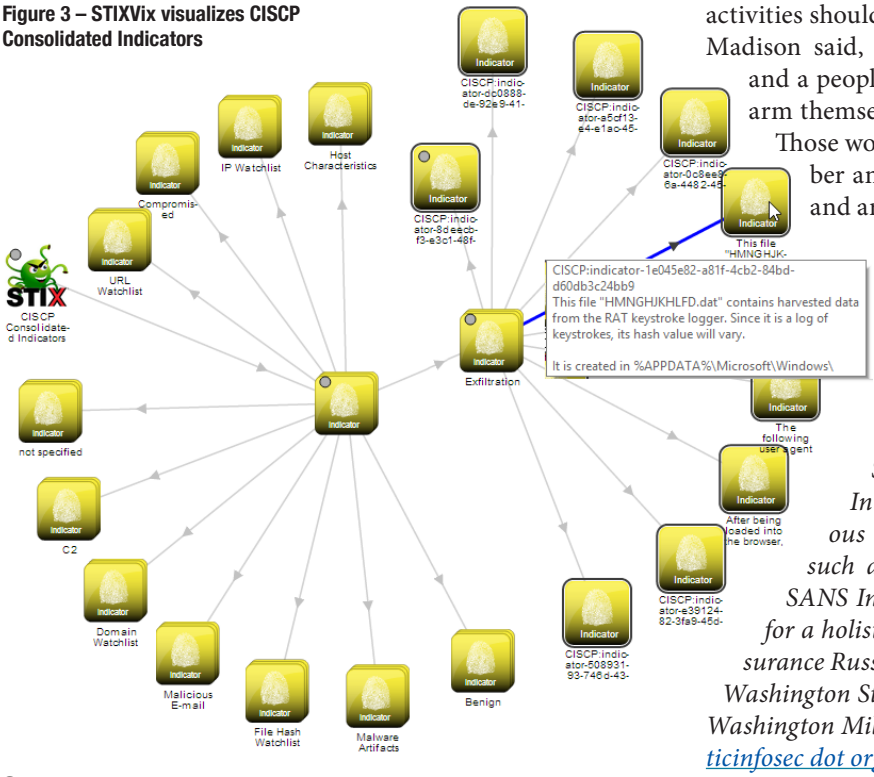
14 http://openioc.org/terms/Common.iocterms.

15 http://holisticinfosec.org/iocs/2a1b3f5d-b6ce-41d9-8500-153a1240a561.ioc.

16 https://github.com/STIXProject/openioc-to-stix.

17 http://holisticinfosec.org/stix/CryptoWallVariant.xml.

Figure 3 – STIXVix visualizes CISCP Consolidated Indicators



activities should be considered essential and required. James Madison said, "Knowledge will forever govern ignorance; and a people who mean to be their own governors must arm themselves with the power which knowledge gives." Those words will ring forever true in the context of cyber and threat intelligence. Use the premise wisely and arm yourself.

Ping me via email if you have questions (russ at holisticinfosec dot org).

Cheers…until next month.

About the Author

Russ McRee manages the Threat Intelligence & Engineering team 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.

STIX-to-HTML

STIX-to-HTML is an XSLT that transforms a STIX 1.0/1.0.1/1.1 document containing metadata and categorized top-level items into HTML for easy viewing. As with STIXViz, download the ZIP, unpack it and grab Saxon,[18] as this tool requires an XSLT 2.0 engine. I downloaded Saxon HE which provides saxon9he.jar as described in STIX-to-HTML guidelines. I simply copied saxon9he.jar right in my STIX-to-HTML directory for ease and convenience. Thereafter I ran `java -jar saxon9he.jar -xsl:stix_to_html.xsl -s:CryptoWallVariant.xml -o:CryptoWallVariant.html`, which resulted in the snippet seen in figure 4, only a partial shot given all the indicators in this STIX file.

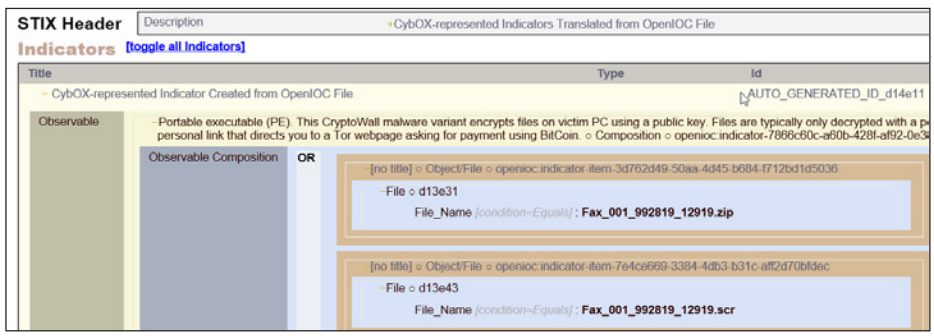


Figure 4 – STIX-to-HTML transforms CryptoWall STIX into an HTML report

You can also customize the STIX-to-HTML transform and add new STIX and CybOX as noted on the wiki associated with the STIX-to-HTML project page.

In conclusion

Great tools from Mandiant and Mitre, all of which make the process of gathering, organizing, and disseminating threat intelligence an easier prospect than some might imagine.

This is an invaluable activity that you should be situating close to or within your security monitoring and incident management programs. If you maintain a security operations center (SOC) or a computer emergency response team (CERT), these

18 http://saxon.sourceforge.net/.