NCCIC

National Cybersecurity and
Communications Integration Center

USING YARA FOR MALWARE DETECTION

This information first appeared in the May/June 2015 edition of the NCCIC/ ICS-CERT Monitor

When NCCIC included a YARA rule in one of its malware advisories, many network defenders called in asking “what is it and how do I use it?”

The effective sharing of intelligence to identify malware has always been a challenge for those working to protect information technology (IT) and industrial control systems (ICS) networks. Traditional hash-based indicators are often not effective with sophisticated attacker groups and automated malware creation toolkits. Hash-based indicators look for exact matches; however, with one simple change of the malware, the indicator no longer works. Defenders can more successfully find malicious files if they focus on identifying malware families (groups of malware that share common code, but are not completely identical) instead of finding exact matches. YARA is a tool that specializes in this type of matching and has become a standard across the malware analysis community.

YARA is a very popular open-source and multi-platform tool (it works with most hosts running Windows, Linux, or Mac operating systems) that provides a mechanism to exploit code similarities between malware samples within a family. The signature files support the documentation of both byte-sequences and string matches that occur in the malware, as well as logic operators that support very robust and precise conditions to reduce the incidence of receiving false positives. NCCIC and other organizations use these signatures to disseminate the intelligence needed by asset owners to defend their networks. For example, the “blackenergy_v3.yara” file included in the Black Energy Alert is a signature file that tells the software what byte-sequences and/or strings on which to alarm. If it finds a match, it will then report to the user. YARA is host based, so users will need to execute the tool via an IT administration tool or manually on each host that they choose to examine. Users should be aware that the application will be analyzing every file in the path that they direct it to examine, so there may be some performance impact to the machine based on the available system resources.

You can download the YARA software and learn more about the tool at http://plusvic.github.io/yara/. If you deploy this to a Windows machine, you can use links on this page to download the precompiled binaries. Then you can simply unzip the downloaded Zip Archive and use a command line similar to this:

```
C:\<Path to Unzipped Archive>\yara32.exe -r <Path to blackenergy_v3.yara File> <Path to whatever you want to scan>
```

Note: You must have admin rights if you wish to scan a whole system.

The “-r” tells the program to recursively search the directories starting from the provided path.

Example:

```
C:\>yara32.exe -r c:\blackenergy_v3.yara c:
```

This example will search the entire “C” drive for anything that matches the signatures provided in the file “blackenergy_v3.yara.” This command should be run as an administrator. If there is a hit on the signature, the output will include a line similar to the following:

```
Black Energy <Path to Suspicious File>
```

Using the freely available YARA tool, defenders are better able to leverage the intelligence available to them, and it also gives them a means of capturing data from their own incident response efforts, which they can use for the tracking of previous threats and for sharing threat information with others.

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center