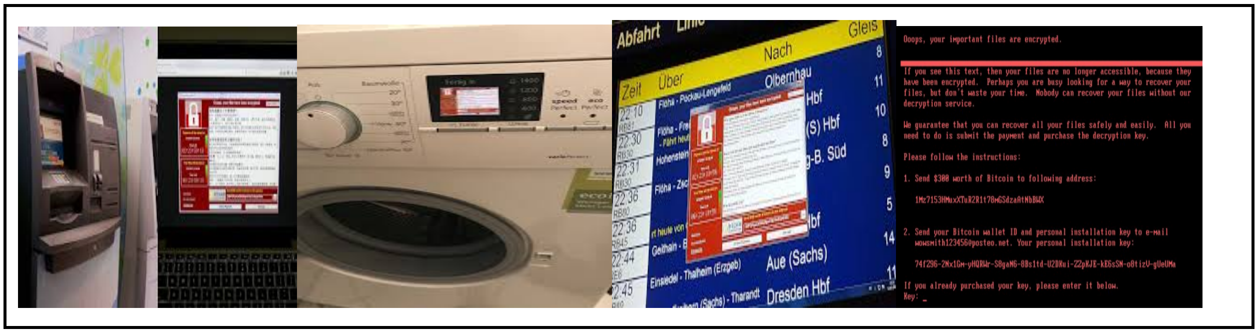
AKTAION v2

Open source machine learning tool for threat detection and active defense.

By Joseph Zadeh & Rod Soto
@josephzadeh / @rodsoto

The continuous success of ransomware campaigns now combined with lateral movement/destructive code, shows an adversarial shift towards payloads that produce quick rewards in massive distributions. Recent successful campaigns show as well that ransomware is capable of bypassing current controls and create real life harm to governments, corporations and individuals. Ransomware in combination with other payloads has become a very powerful weapon to which there seems to be no effective way to stop and it targets literally anything from washers, dryers, train stations, hospitals, nuclear power/utility plants, etc.

Fig 1. Ransomware infected ATM, Washer, Train station screen, Hospital computer desktop



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

Recent campaigns have witnessed affected victims simply paying ransom or even powering off assets as a way to stop infestation. The modus operandi has however stayed similar. Malicious payload gets sent via distribution mean (E-mail, Website), and this payload delivery it's usually wrapped under a misleading message or trustworthy appearance (Software Update, Office Document, Alert/Warning), targeting user's trust in order to bypass security controls.

Moreover there are indications that Ransomware in combination with lateral movement/privilege escalation/destructive payloads are being used by state actors in a way to increase damage, entrenchment and also obfuscation when targeting their victims. The recent 2017 campaign featuring what was believed to be Petya ransomware, turned out to be multiple "Petya" looking like in appearance but behind the presented screen the payloads were different and with specifically designed functions per target.

Authors believe that by approaching ransomware using machine learning techniques and dissecting its exploit chain and multi contextual items in what we call "Micro Behaviors" does indeed provide a more effective way of detecting and acting on ransomware attacks. By applying a framework of analysis based on what we define as the "Lambda Defense", organizations can detect, and contain a ransomware campaign more effectively.

Micro Behaviors and contextual indicators

Micro Behaviors are basic units that are present in a threat, these basic units can be dissected and labeled from most common log information or network captures. Indeed many of current logging and network monitoring technologies, provide data where these micro behaviors can be found in large quantities and historical records.

By labeling these micro behaviors and applying machine learning techniques supported by the lambda defense architecture, which consists of the use of big data technologies applied to the handle and analysis of large quantities of data, authors believe the odds of detecting and stopping malware are higher than using traditional static based defense technologies. Authors believe the most effective way to detect ransomware is by focusing on the delivery of it. This delivery process of ransomware as explained above also contains micro behaviors that can be attributed to "Phishing". Phishing is a type of attack that involves sending malicious emails usually purporting to be from a known or trustworthy source. Aktaion version 2 can certainly catch phishing attempts as well as they are usually part of the Ransomware payload delivery exploit chain.

Micro Behaviors present in Ransomware

Aktaion version 2 continues the analysis of Ransomware Micro Behaviors including the following:

- Payload delivery. Focused on traffic to malicious sites and the related indicators when malicious code is served. Including things such as URI entropy, redirects, domain generated by algorithms (DGAs), types and sequences of MIME content presented to victim during payload delivery.

- Call backs (Phone home) patterns, including user agent, URI strings, HTTP "GET" or "POST" requests, DNS queries, URI strings, frequency of call-backs, periodicity of connections.

- Covert Channel indicators, such as non HTTP traffic (HTTPS), and non DNS traffic present during such communications.

In version 2 Aktaion adds the following micro behaviors.

- Entropy in URI/URL (number of dots, special characters, URL crazy)
- Whois (registrar with bad rep / geolocation / bulletproof hosting
- URL Shorteners (Tiny URL, bit.ly, etc)
- Spelling errors, passwords fields
- Presence of iframes, javascript, pagerank?, source of images
- Presence of .exe .pdf .bat .ps1 .ps .bin .bat .jar .bin .zip

With the addition of these new micro behaviors Aktaion v2 aims to cover as many identifiable behaviors as possible from a simple pcap capture. Once the models have been trained with benign data and malicious data, based on the above criteria the tool will produce the following:

- Malicious URIs/URLs detected = I.E evil.com
- Indicator match of the criteria used by learner (Ransomware delivery/Phishing behavior)
- Grade of confidence
- Prompt for action to create SNORT signature (Phishing)
- Prompt for action to execute SSH - GPO (prevents Ransomware exe execution)

Aktaion is an open source tool and can be customized as well, it can take input from different sources, including static signature based technologies (SIEM, IDS, IPS).

The tool

Github link

https://github.com/jzadeh/aktaion

Requirements

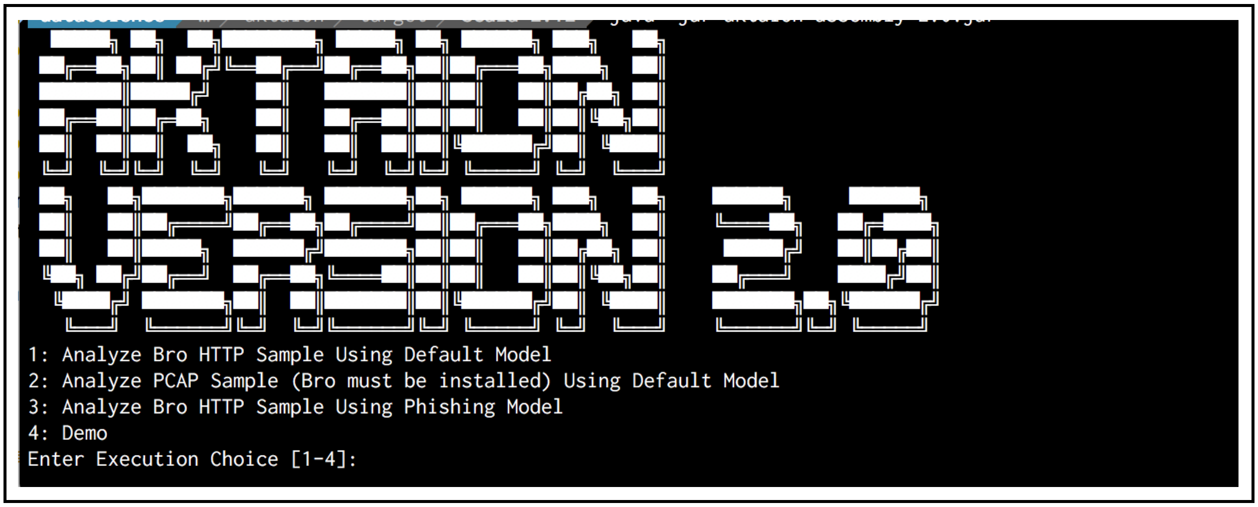
Python 2.6, 3.7
Java 1.8
Bro IDS

Aktaion v2 is currently being ported to Python, in order to make it easier to use and interoperable with any operating system that supports python language. Once the tool is executed it presents operator with 4 options, including analyzing a Bro HTTP sample using default model (ransom delivery), analyze a pcap capture with default model, analyze Bro HTTP sample using PHISHING model and demo, using real benchmark benign data and malicious data for training.

Active Defense

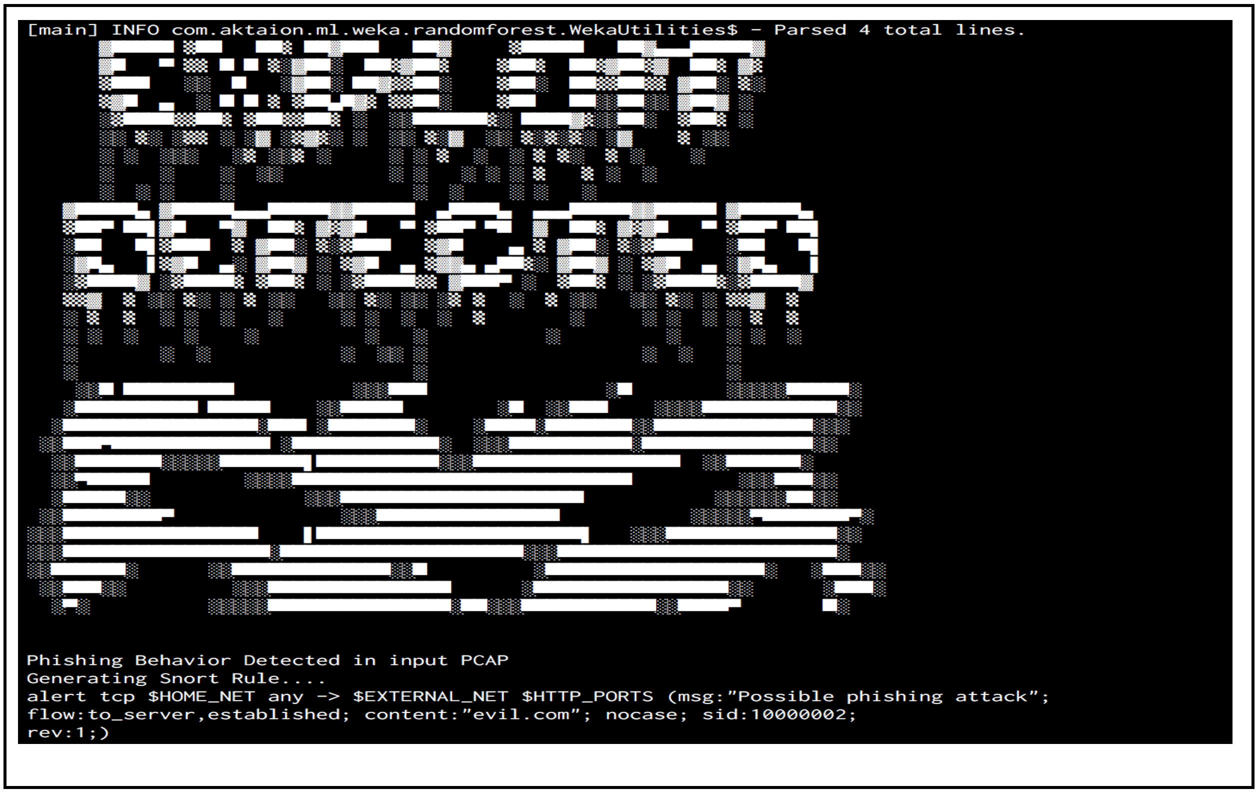
One of the goals of Aktaion v2 is to produce active defense measures to help operators take action upon threat detection. In Aktaion v2 in addition to provide the option for a GPO to prevent execution of malicious file related to ransomware delivery, Aktaion v2 provides a generic SNORT alert after detecting Phishing behavior.

Fig 2. Initial menu



```
1: Analyze Bro HTTP Sample Using Default Model
2: Analyze PCAP Sample (Bro must be installed) Using Default Model
3: Analyze Bro HTTP Sample Using Phishing Model
4: Demo
Enter Execution Choice [1-4]:
```

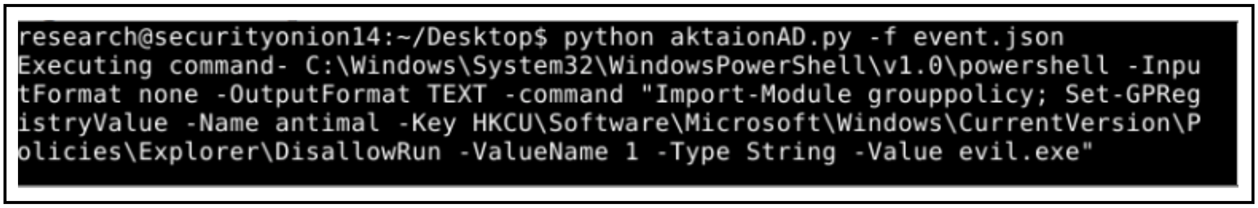
Fig 3. Phishing detection and SNORT alert



```
[main] INFO com.aktaion.ml.weka.randomforest.WekaUtilities$ - Parsed 4 total lines.
```

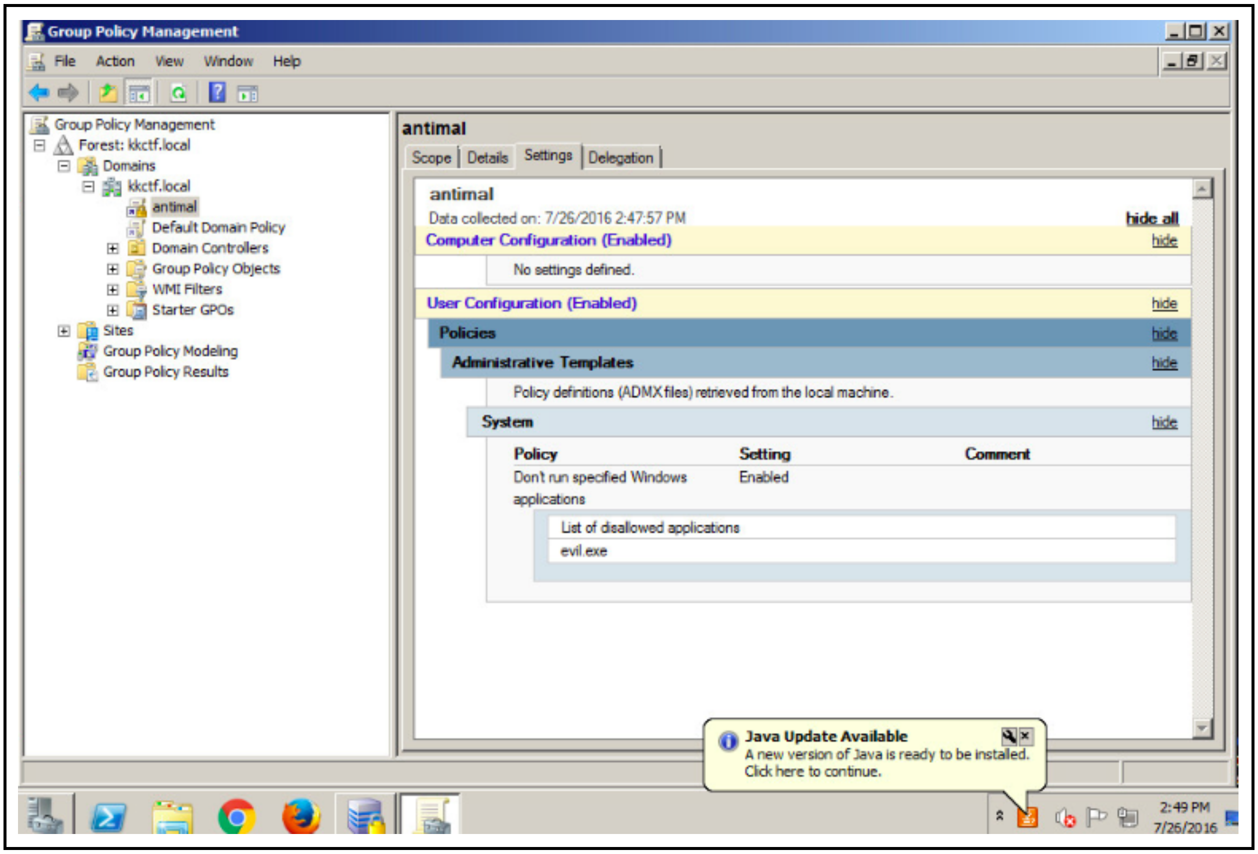
```
Phishing Behavior Detected in input PCAP
Generating Snort Rule....
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Possible phishing attack";
flow:to_server,established; content:"evil.com"; nocase; sid:10000002;
rev:1;)
```

Fig 4. Example of GPO script based of malicious executable delivery detection.



```
research@securityonion14:~/Desktop$ python aktaionAD.py -f event.json
Executing command- C:\Windows\System32\WindowsPowerShell\v1.0\powershell -Inpu
tFormat none -OutputFormat TEXT -command "Import-Module grouppolicy; Set-GPReg
istryValue -Name antimal -Key HKCU\Software\Microsoft\Windows\CurrentVersion\P
olicies\Explorer\DisallowRun -ValueName 1 -Type String -Value evil.exe"
```

Fig 5. GPO result at target AD server



antimal

antimal

Data collected on: 7/26/2016 2:47:57 PM

Computer Configuration (Enabled)

No settings defined.

User Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local machine.

System

Policy	Setting	Comment
Don't run specified Windows applications	Enabled	

List of disallowed applications
evil.exe

Java Update Available

A new version of Java is ready to be installed. Click here to continue.

References

https://www.python.org/
https://github.com/jzadeh/aktaion/blob/master/documentation/AktaionvWhitePaperBlackHat2016.pdf
https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/#4ed15ef0532e