RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: PART2-T08

Confessions of a Sandbox: How AI is Disrupting Automated Threat Analysis

Marian Radu
Senior Director, Data Science
CrowdStrike
@radu_marian

Liviu Arsene
Director of Threat Research and Reporting
CrowdStrike
@liviuarsene

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Agenda

- Automated threat analysis
- Advanced threats and bypassing techniques
- The power of machine learning
- Takeaways

RSAConference2022

Automated Threat Analysis

Automated Threat Analysis

The Sandbox:

A sandbox is a closed system that enables security professionals to watch the malware in action without the risk of letting it infect their system or escape into the enterprise network.

- Mimics an end-user operating environment
- Prevents accidental exposure to potential threats

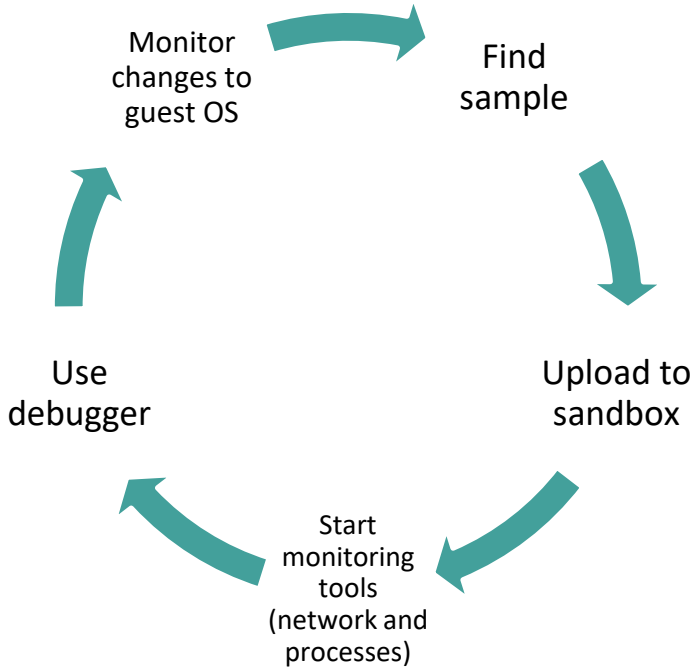
Automated Threat Analysis

The Tools

- Static analysis tools
- Network monitoring tools
- Process monitoring tools
- Debbuggers
- System level API hooks
- Machine learning
- YARA rules
- Etc.

Automated Threat Analysis

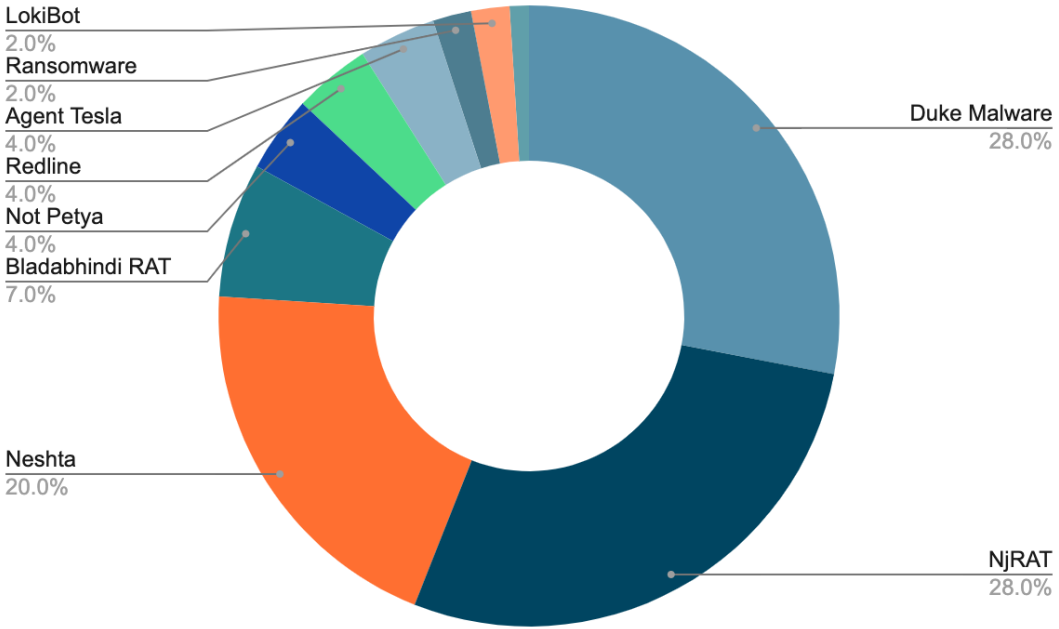
The Automation



RSAConference2022

Bypass Techniques Used by Advanced Threats

Top 10 Malware Families Based on Hybrid Analysis Submissions



CROWDSTRIKE

Bypass Techniques Used by Advanced Threats

Masquerading (T1036)

- Manipulating features of their artifacts to make them appear legitimate or benign to users and/or security tools
- Secondary payloads that use (mis)spelling of common filenames
- Using lolbins (certutil, bitsadmin, etc.)

Software Packing (T1027)

- Used for compressing or encrypting an executable
- Decompressing code in memory (e.g. URLs unpacked in memory)

Lateral Tool Transfer (T1570)

- Transfering tools or other files between systems in a compromised environment
- Network connections to URLs to download and drop additional payloads, such as bitsadmin to download files

RSAConference2022

The Power of Machine Learning

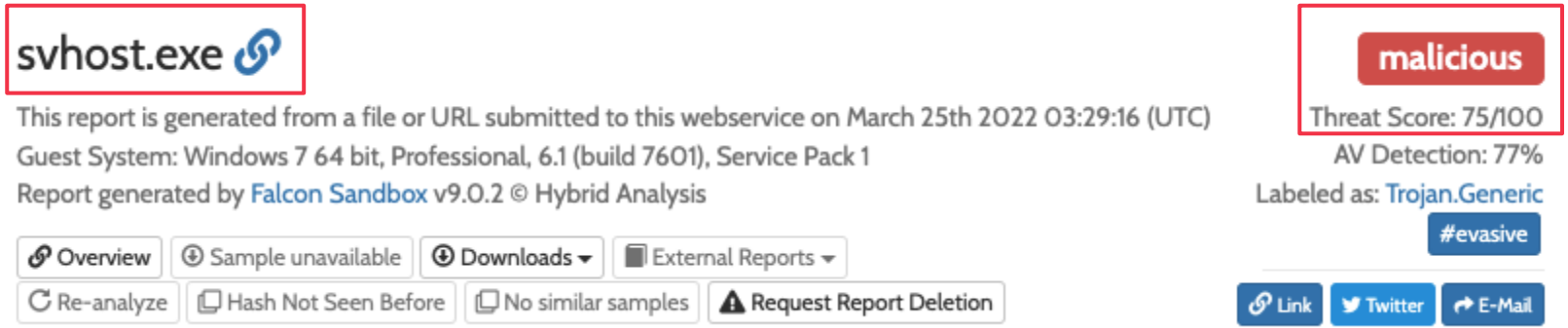
Disrupting Automated Threat Analysis

Disrupting Traditional Automated Threat Analysis

- Fast and reliable scanning results for:
  - binaries
  - memory dumps
  - URLs
- Comprehensive detonation report for IOCs

The Power of Machine Learning

Masquerading technique impersonating a legitimate binary



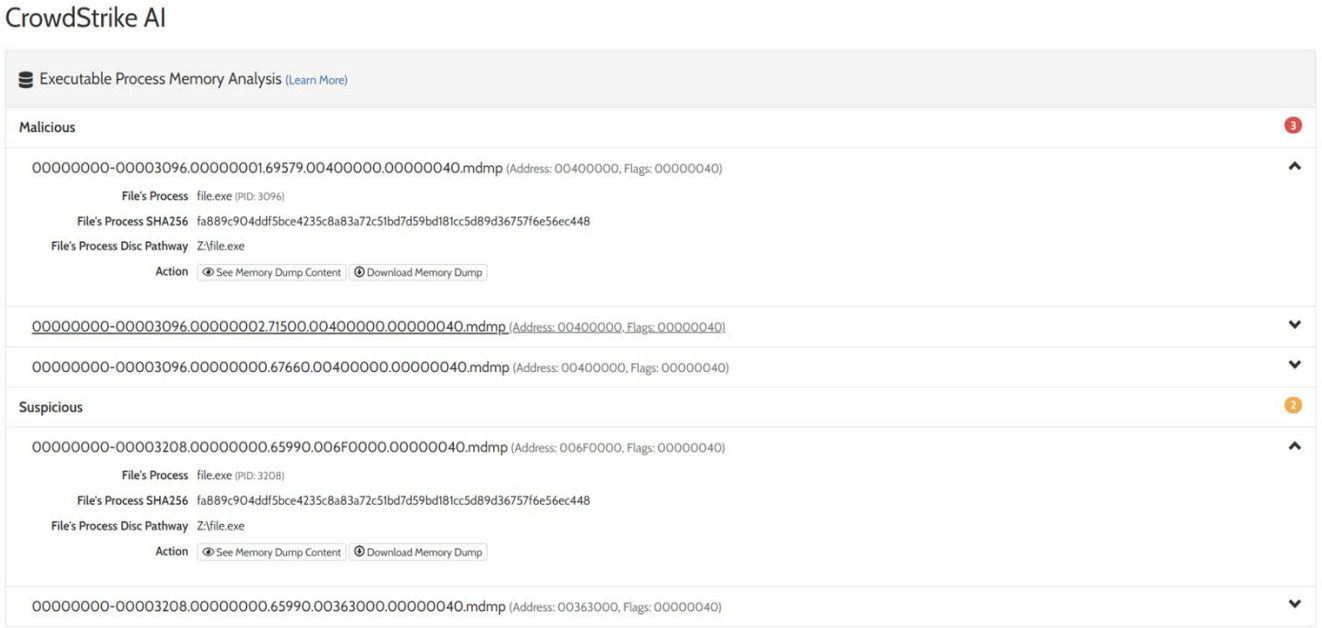
The Power of Machine Learning

Masquerading and Lolbin techniques used to drop additional tools

CROWDSTRIKE

The Power of Machine Learning

Memory dump analysis using CrowdStrike AI



CROWDSTRIKE

The Power of Machine Learning

Memory dump analysis using CrowdStrike AI

Data Collection → Feature Extraction → Model Training → Prediction

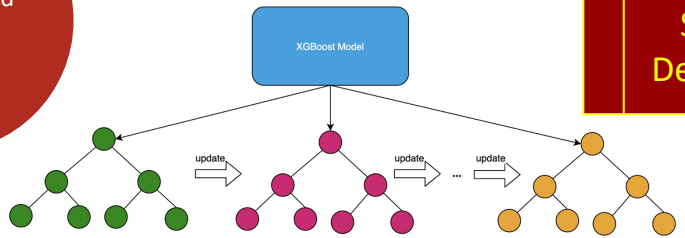
Memory Dumps

Pre-trained Embeddings

Opportunistic instruction decoding

Signals hand picked by experts

Transfer Learning



Memory Dumps from Sandbox Detonations

CROWDSTRIKE

The Power of Machine Learning

Network activity analysis using CrowdStrike AI

Applying CrowdStrike AI to URLS extracted from:

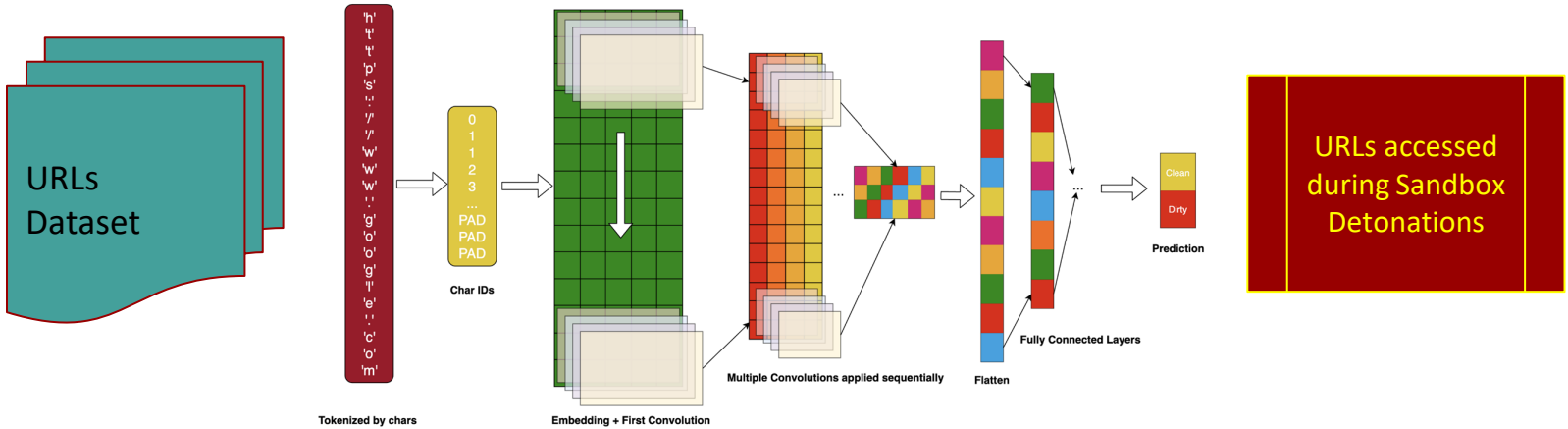
- Extracted Strings section
- Network analysis section
- Submitted URLs (submitted by users for analysis)

CROWDSTRIKE

The Power of Machine Learning

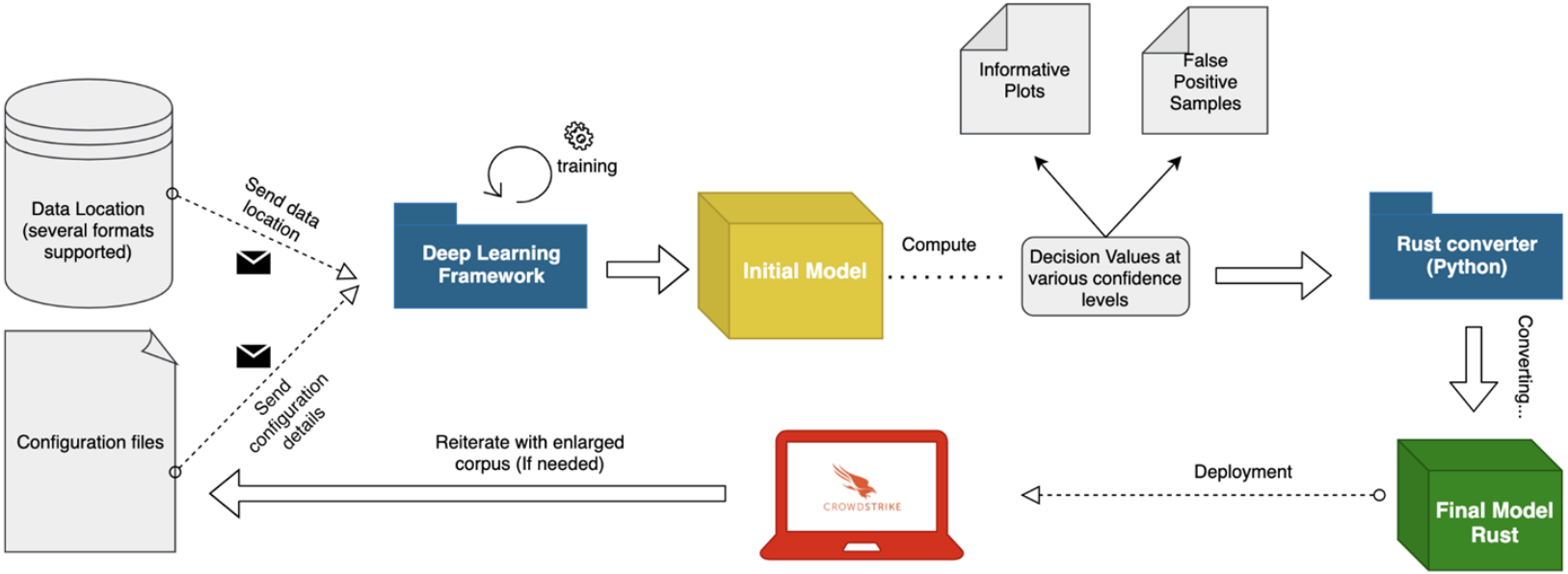
URLs analysis using CrowdStrike AI

Data Collection | Model Training | Prediction



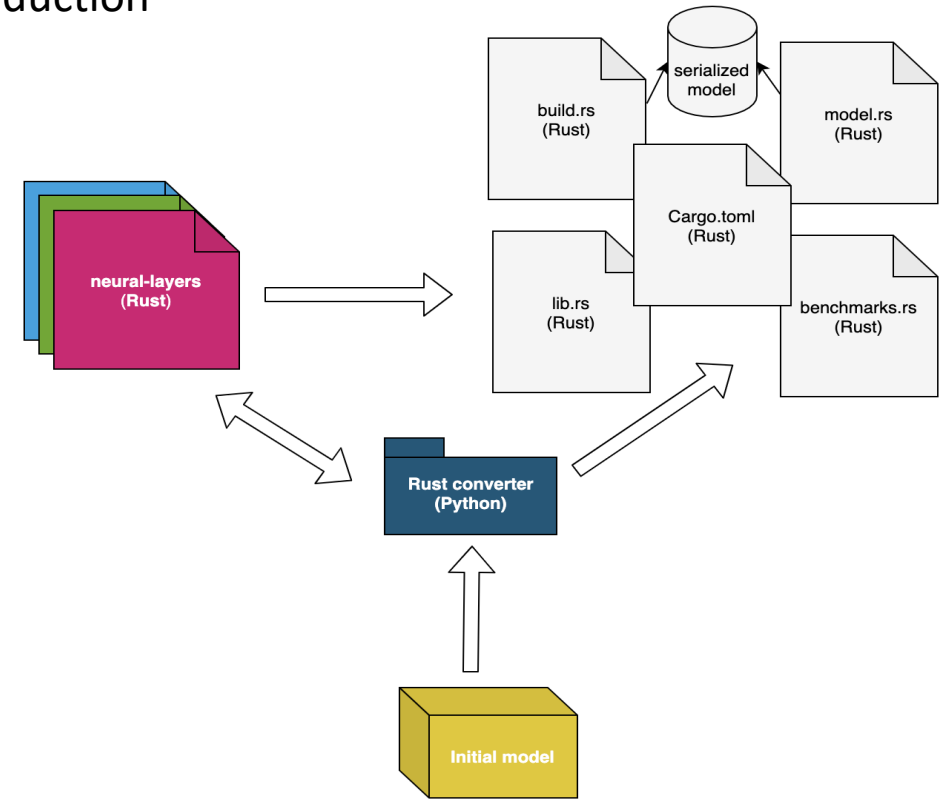
The Power of Machine Learning

Performance Optimizations



The Power of Machine Learning

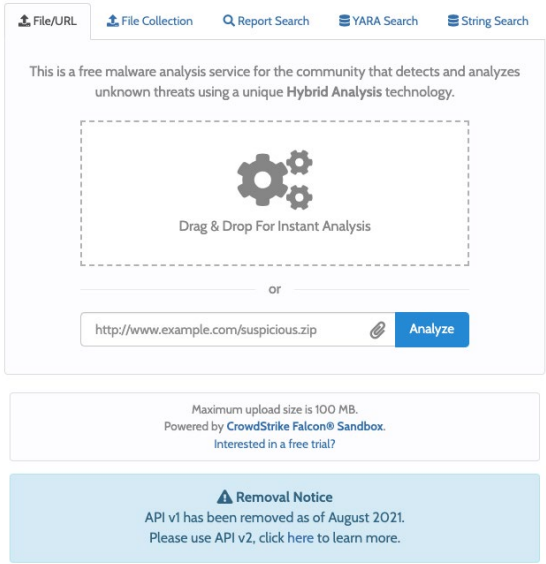
Attack Surface Reduction



RSAConference2022

Video Demo

Disrupting Traditional Automated Threat Analysis



- Publicly available free tool for researchers and analysts community
- Supports URLs, Windows 7 32/64 bit, Linux, and Android static analysis
- QuickScan
  - Machine learning static analysis
  - Processes over 700K files daily
- Detonation report generator and post detonation actions
  - “Heuristic” Sandbox Threat Score
  - Behavioral signatures (hooks, handles, mutant, network, registry, binary, certificate, api, etc.)
  - Machine Learning for memory analysis, ransomware, and URLs
  - YARA processing
  - Network PCAP files
  - Screenshots
  - MITRE ATT&CK mapping
  - Process tree
  - Dropped files
  - etc.

CROWDSTRIKE

How do Researchers Feel About It?

"…what Hybrid has, what others haven't, is the reporting and the ease of which I can get samples out of it. From a pure IOC point of view, that's where Hybrid really stands up." - Mike, Security Architect

"The bit that I liked about hybrid, particularly was being able to YARA research on things and that's really good," - Nick, Security Architect

"With hybrid analysis everything was simple, I went into the documentation, I took my API key, I took the client from GitHub and I cloned it. Everything just works, no problem…" - John, Engineer

"And that is awesome that I can go in there and download samples. I absolutely love that," - Steve, IT Administrator

"All of the samples we've sent through have given us the MITRE attack labels that we need" - Joe, Test Engineer

CROWDSTRIKE

RSAConference2022

Takeaways

Takeaways

- Traditional automated threat analysis is more about IOCs than malicious assessment
- Advanced threats use sophisticated tactics to bypass traditional automated threat analysis tools
- Machine learning augments automated threat analysis, offering quick assessment and deep insights into malicious behaviour
- In the end, Machine Learning disrupts automated threat analysis by increasing its efficacy: easier, faster, more accurate … and free.

CROWDSTRIKE

RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART2-T08**

Thank You

Confessions of a Sandbox: How AI is Disrupting Automated Threat Analysis

Marian Radu
Senior Director, Data Science
CrowdStrike
@radu_marian

Liviu Arsene
Director of Threat Research and Reporting
CrowdStrike
@liviuarsene

Backup Slides

MITRE ATT&CK Technique Detection and Mapping

Execution

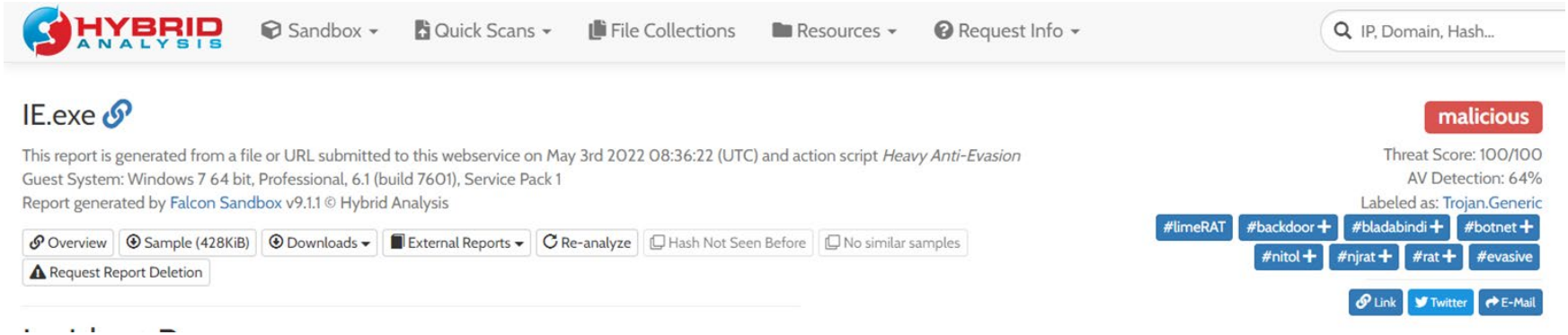
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1204.002	Malicious File	• Execution	An adversary may rely upon a user opening a malicious file in order to gain execution. Learn more	• Document spawns new processes		
T1204	User Execution	• Execution	An adversary may rely upon specific actions by a user in order to gain execution. Learn more		• Contains embedded VBA macros with suspicious keywords • Contains embedded VBA macros with interesting strings	• Contains embedded VBA macros
T1059.003	Windows Command Shell	• Execution	Adversaries may abuse the Windows command shell for execution. Learn more			• Runs shell commands

Persistence

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1137	Office	• Persistence	Adversaries may leverage Microsoft	• Contains embedded VBA		• Contains embedded

Backup Slides

User tags



Backup Slides

Suricata alerts

Suricata Alerts

Event	Category	Description	SID
local -> 8.8.8.8:53 (UDP)	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.ddns .net	2028675 %}
local -> 8.8.8.8:53 (UDP)	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.ddns .net	2028675 %}
54.254.238.33 -> local:49185 (TCP)	-	-	- %}
54.254.238.33 -> local:49185 (TCP)	Potentially Bad Traffic	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response	2021076 %}
54.254.238.33 -> local:49186 (TCP)	-	-	- %}
54.254.238.33 -> local:49186 (TCP)	Potentially Bad Traffic	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response	2021076 %}
local -> 8.8.8.8:53 (UDP)	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.ddnsking .com	2028676 %}
local -> 8.8.8.8:53 (UDP)	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.ddnsking .com	2028676 %}
local -> 8.8.8.8:53 (UDP)	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.3utilities .com	2028677 %}
local -> 8.8.8.8:53 (UDP)	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.3utilities .com	2028677 %}
local -> 8.8.8.8:53 (UDP)	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.bounceme .net	2028678 %}

Backup Slides