7a78e1a7efed4513d629e7b4d95157fee4f8ecf65e9eaa39bbb109d36164a0bd

Sign in Sign up

1 / 71

Community Score

1/71 security vendor flagged this file as malicious

Reanalyze Similar More

7a78e1a7efed4513d629e7b4d95157fee4f8ecf65e9eaa39bbb109d36164a0bd

7a78e1a7efed4513d629e7b4d95157fee4f8ecf65e9eaa39bbb109d36164a0bd.exe

peexe runtime-modules long-sleeps direct-cpu-clock-access checks-user-input overlay detect-debug-environment

Size 2.64 MB

Last Analysis Date a moment ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Bkav Pro	W32.AIDetectMalware	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Arctic Wolf	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected

Applications Places System Mon Apr 21, 18:41

MalwareBazaar | Downloa × VirusTotal - File - 7a78e1a × ATT&CK Data & Tools | M × PROMETHIUM, StrongPit × APT29 Overview and TTPs ×

a39bbb109d36164a0bd/

rning Resources

Parrot Terminal

File Edit View Search Terminal Help

```
[---]       Homepage: https://www.trustedsec.com       [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

          Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

domain, URL or file hash has been identified on any platform from a .ch - and happy hunting 🔍

Hunting Alerts Access Data FAQ About Login

95157fee4f8ecf65e9eaa39bbb109d36164a0bd

ave understood what you are doing and that MalwareBazaar can not

Terms and Conditions | Terms of Use | Privacy Policy | Cookie Policy

Menu MalwareBazaar | Do... mobile-attack-v16.1-g... Parrot Terminal Parrot Terminal

```
[---]       The Social-Engineer Toolkit (SET)       [---]
[---]       Created by: David Kennedy (ReL1K)       [---]
                      Version: 8.0.3
                   Codename: 'Maverick'
[---]       Follow us on Twitter: @TrustedSec       [---]
[---]       Follow me on Twitter: @HackingDave      [---]
[---]      Homepage: https://www.trustedsec.com     [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

  The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

  It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

```
[---]       The Social-Engineer Toolkit (SET)       [---]
[---]       Created by: David Kennedy (ReL1K)       [---]
                      Version: 8.0.3
                   Codename: 'Maverick'
[---]       Follow us on Twitter: @TrustedSec       [---]
[---]       Follow me on Twitter: @HackingDave      [---]
[---]      Homepage: https://www.trustedsec.com     [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

  The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

  It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

```
                Codename: 'Maverick'
[---]          Follow us on Twitter: @TrustedSec          [---]
[---]          Follow me on Twitter: @HackingDave         [---]
[---]         Homepage: https://www.trustedsec.com        [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set>
```

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>

```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) HTA Attack Method

 99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>
```

```
                Codename: 'Maverick'
[---]          Follow us on Twitter: @TrustedSec          [---]
[---]          Follow me on Twitter: @HackingDave         [---]
[---]       Homepage: https://www.trustedsec.com          [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set>
```

```
  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set> 5
```



```
  Social Engineer Toolkit Mass E-Mailer

  There are two options on the mass e-mailer, the first would
  be to send an email to one individual person. The second option
  will allow you to import a list and send it to as many people as
  you want within that list.

  What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:mailer>
```

```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) HTA Attack Method

 99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>
```