Metasploit Pro

Setting Up a USB Key Drop

What is a USB Key Drop?

USB key dropping is a social engineering tactic that can be used to obtain sensitive information or remote access to a human target's computer. A social engineer or penetration tester may want to leverage USB key drops to raise security awareness, ensure adherence to security procedures, and improve defense strategies within an organization.

Typically, the attacker places a malicious file or executable onto the USB key and drops the key off in a high traffic area like the breakroom. If someone finds the key and installs the device on their system, the malicious file will run if the autorun feature is implemented or it will run when the person clicks on the executable file. When the file runs, it delivers a payload that could potentially open a backdoor on the human target's machine. If a session successfully opens on a victim's machine, an attacker can take control of it to attack other machines on the network, capture data, and escalate privileges.

What Do I Need to Set Up a USB Key Drop?

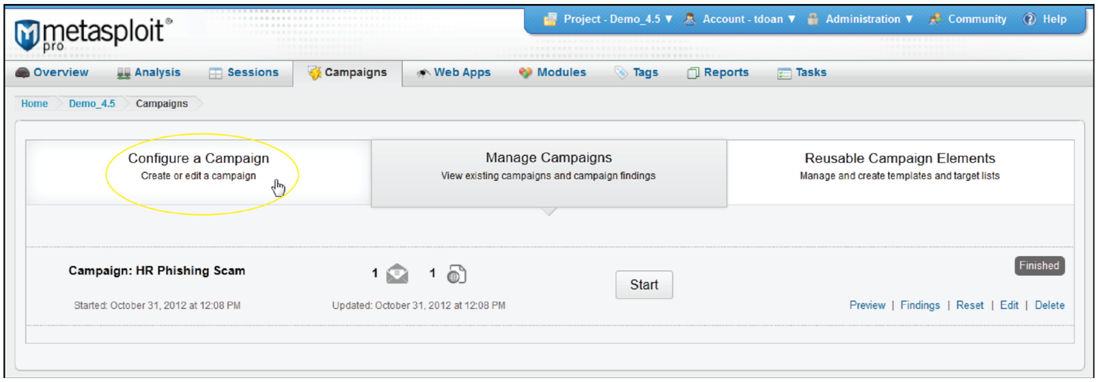
Component	Description
Campaign	A logical grouping of components that you need to perform a social engineering attack, such as a web page or e-mail. Each social engineering attack is configured from within a campaign.
Portable File	A campaign component that generates an execuatable file or file format exploit.
Executable File	A file that delivers a payload to the human target's machine. The payload starts a session on the target's machine and creates a connection back to you.
USB Key	A flash drive that you can use to store, transfer, or back up data. In social engineering, you can use a USB key as a delivery mechanism for file format exploits and excecutable files.
Listener Callback IP	The IP address that the target machine connects back to. Metasploit Pro assigns the IP address of the Metasploit instance as the callback IP address.
Listener Callback Port	The listener port that the attacking machine listens on for incoming connections. Metasploit Pro automatically searches through a range of ports and assigns the first available port that it finds as the callback port.

What Are the General Steps to Create a USB Key Drop?

Task 1: Create a custom campaign.
Task 2: Add a portable file component to the campaign.
Task 3: Name the portable file component and specify the name for the executable file.
Task 4: Download the executable file and save it to your computer.
Task 5: Launch the campaign.
Task 6: Transfer the executable to a USB key.
Task 7: Distribute the USB key to human targets.
Task 8: Wait for incoming connections.

Setting Up a USB Key Drop

1. Open the default project.
2. Select **Campaigns** from the Tasks bar. The **Manage Campaigns** page appears.
3. Click the **Configure a Campaign** tab.

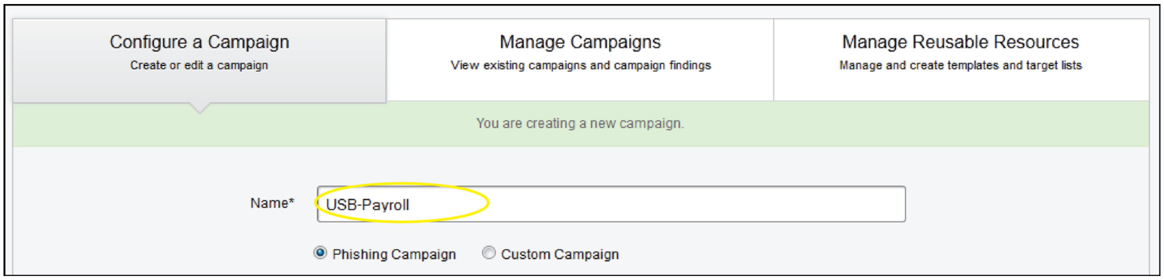


Campaign: HR Phishing Scam 1 1

Started: October 31, 2012 at 12:08 PM

Updated: October 31, 2012 at 12:08 PM

4. Enter a descriptive name for the campaign. For example, **USB-Payroll** helps you easily identify the campaign type and the executable file name.

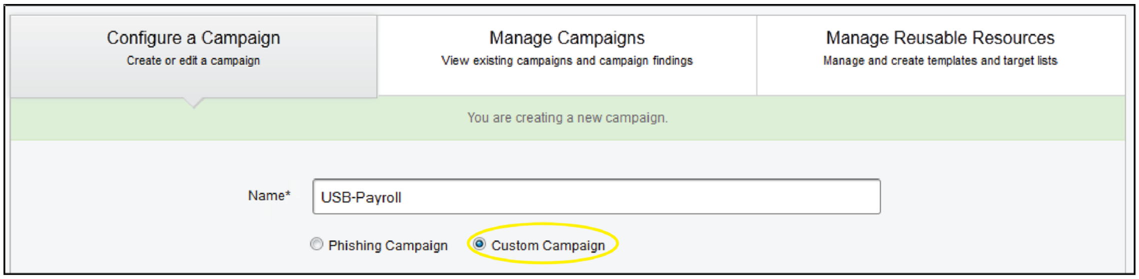

Configure a Campaign
Create or edit a campaign
Manage Campaigns
View existing campaigns and campaign findings
Manage Reusable Resources
Manage and create templates and target lists

You are creating a new campaign.

Name* USB-Payroll

● Phishing Campaign ○ Custom Campaign

5. Select the **Custom Campaign**.

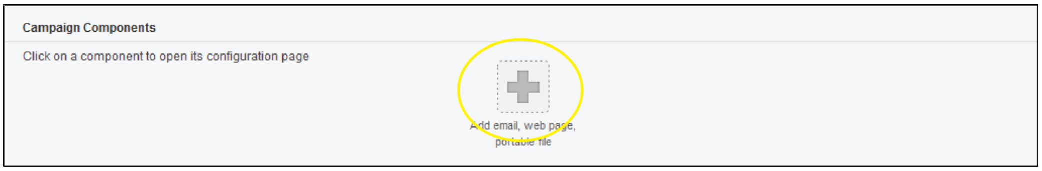

Configure a Campaign
Create or edit a campaign
Manage Campaigns
View existing campaigns and campaign findings
Manage Reusable Resources
Manage and create templates and target lists

You are creating a new campaign.

Name* USB-Payroll

○ Phishing Campaign ● Custom Campaign

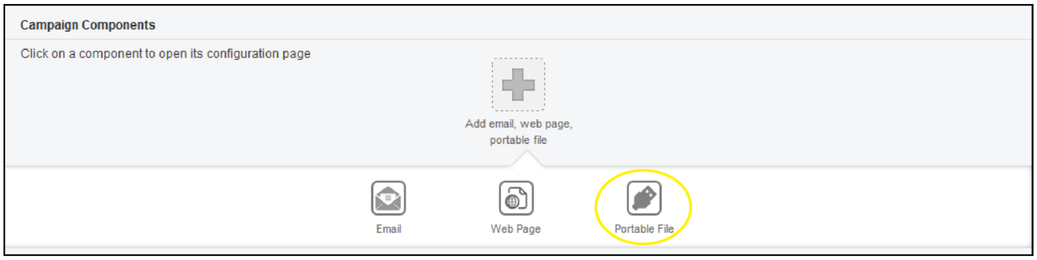
6. Click the **Add email, web page, portable file** button. A set of campaign components appears.



Campaign Components

Click on a component to open its configuration page

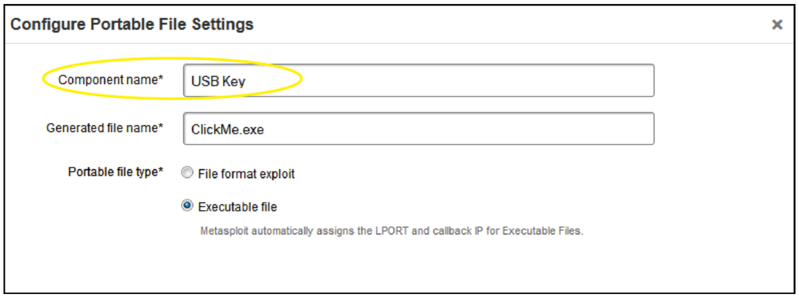
7. Click the **Portable File** button. The portable file configuration page appears. Default values have been defined for the portable file and the executable file. If you do not want to customize the names of these files, you can skip to step 10.



Campaign Components

Click on a component to open its configuration page

8. Enter a unique name for the portable file component. This name displays under the portable file icon on the campaign configuration page.

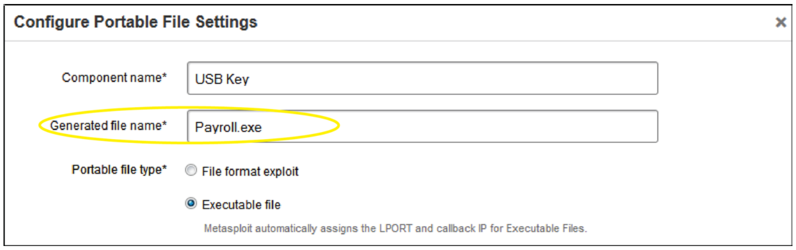


Configure Portable File Settings

Component name*	USB Key
Generated file name*	ClickMe.exe
Portable file type*	○ File format exploit ● Executable file

Metasploit automatically assigns the LPORT and callback IP for Executable Files.

9. Enter a name for the executable file. This is the file name that the human target sees when they look at the contents of the USB drive. You want to give the file a name that entices the user to click on it. For example, a name like “Payroll” or “Company Bonuses” may work well.



Configure Portable File Settings

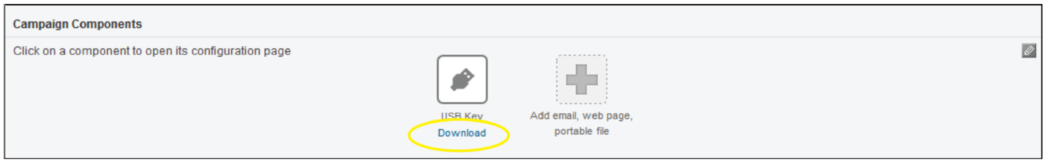
Component name*	USB Key
Generated file name*	Payroll.exe
Portable file type*	○ File format exploit ● Executable file

Metasploit automatically assigns the LPORT and callback IP for Executable Files.

10. Verify that **Executable file** is selected as the **Portable file type**. The executable delivers a reverse TCP payload to the human target and attempts to connect back to the attacking machine.

11. Click **Save** to save the executable.

12. When the **Configure a Campaign** area reappears, you will see a **Download** link located beneath the USB Key icon. Click the **Download** link and save the executable file to a location on your local machine. The Desktop or Downloads folder is a good location.



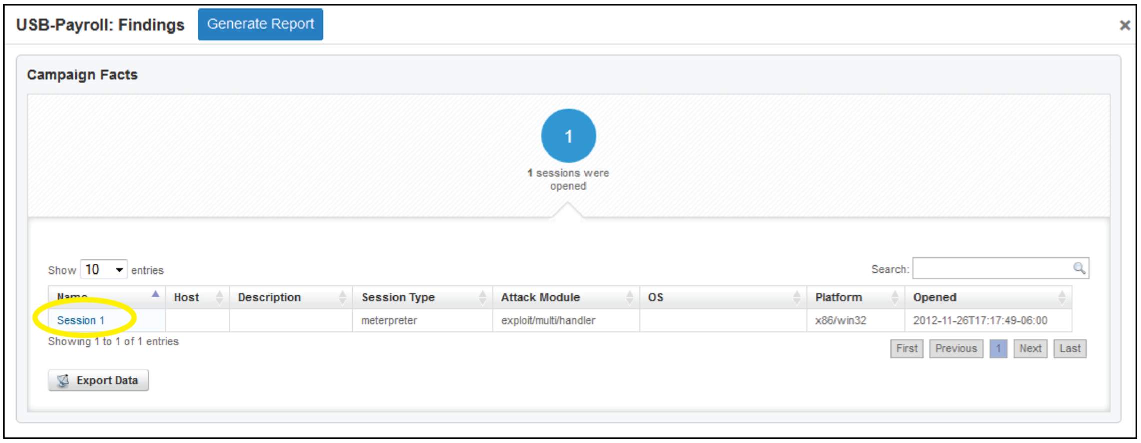
Campaign Components

Click on a component to open its configuration page

13. Insert your USB key into your USB port and move the executable over to a USB drive.

14. Click the **Launch Campaign** button to start the campaign. The campaign must be online for you to be able to obtain a session on a target machine.

Immediately after you start the campaign, the Campaign Findings window appears. This window displays the current number of sessions that the campaign was able to obtain on target machines. If a session successfully opens on the human target's machine, you can click on the session name to see a list of actions that you can perform against the machine.



USB-Payroll: Findings

Campaign Facts

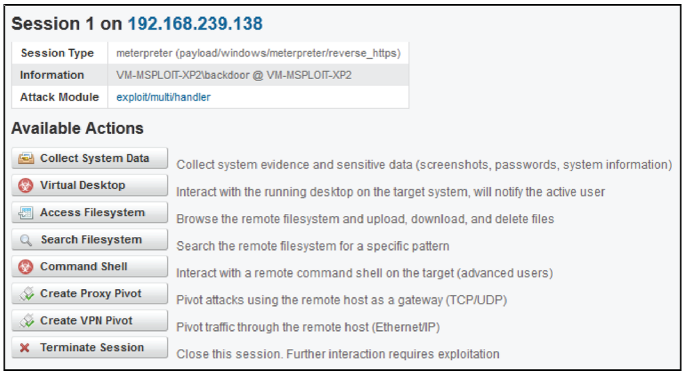
1 sessions were opened

Show 10 entries

Name	Host	Description	Session Type	Attack Module	OS	Platform	Opened
Session 1			meterpreter	exploit/multi/handler		x86/win32	2012-11-26T17:17:49-06:00

Showing 1 to 1 of 1 entries

For example, you may be able to do things like collect screenshots and passwords from the exploited machine or you may be able to access its file system.



Session 1 on 192.168.239.138

Session Type	meterpreter (payload/windows/meterpreter/reverse_https)
Information	VM-MSPLOIT-XP2\backdoor @ VM-MSPLOIT-XP2
Attack Module	exploit/multi/handler

Available Actions

Collect System Data	Collect system evidence and sensitive data (screenshots, passwords, system information)
Virtual Desktop	Interact with the running desktop on the target system, will notify the active user
Access Filesystem	Browse the remote filesystem and upload, download, and delete files
Search Filesystem	Search the remote filesystem for a specific pattern
Command Shell	Interact with a remote command shell on the target (advanced users)
Create Proxy Pivot	Pivot attacks using the remote host as a gateway (TCP/UDP)
Create VPN Pivot	Pivot traffic through the remote host (Ethernet/IP)
Terminate Session	Close this session. Further interaction requires exploitation

Dropping off the USB Key

Now, you are ready to drop off the USB key. You should look for places where people are likely to put things down and forget them, like near the coffee pot in the breakroom or on the sink in the bathroom. People will likely want to view the contents of the USB key to identify the owner and to return the key to the rightful person.