

TryHackMe: Incident handling with Splunk

Link: <https://tryhackme.com/r/room/splunk201>

Neste exercício iremos investigar um ataque cibernético de deface no site de uma organização. A solução SIEM é Splunk e categorizaremos as atividades do atacante nas 7 fases descritas na Cyber Kill Chain.

A grande corporação Wayne Enterprises recentemente enfrentou um ataque cibernético em qual os atacantes invadiram sua rede, acharam seu servidor web, e conseguiram realizar um ataque de deface no website <http://www.imreallynotbatman.com>. O site agora mostra a marca registrada dos atacantes, com a mensagem “YOUR SITE HAS BEEN DEFACED”.



Figura 1 - Site que sofreu o deface.

Logs do Splunk estão sendo ingeridos de webserver/firewall/Suricata/Sysmon.

Algumas fontes de logs interessantes são:

- wineventlog
- winRegistry
- XmlWinEventLog
- fortigate_utm
- iis
- Nessus:scan
- Suricata
- stream:http
- stream: DNS
- stream:icmp

Reconnaissance Phase

Obs: Caso as pesquisas nesta fase não estejam funcionando para você, talvez seja necessário mudar a data das pesquisas para “All time”.

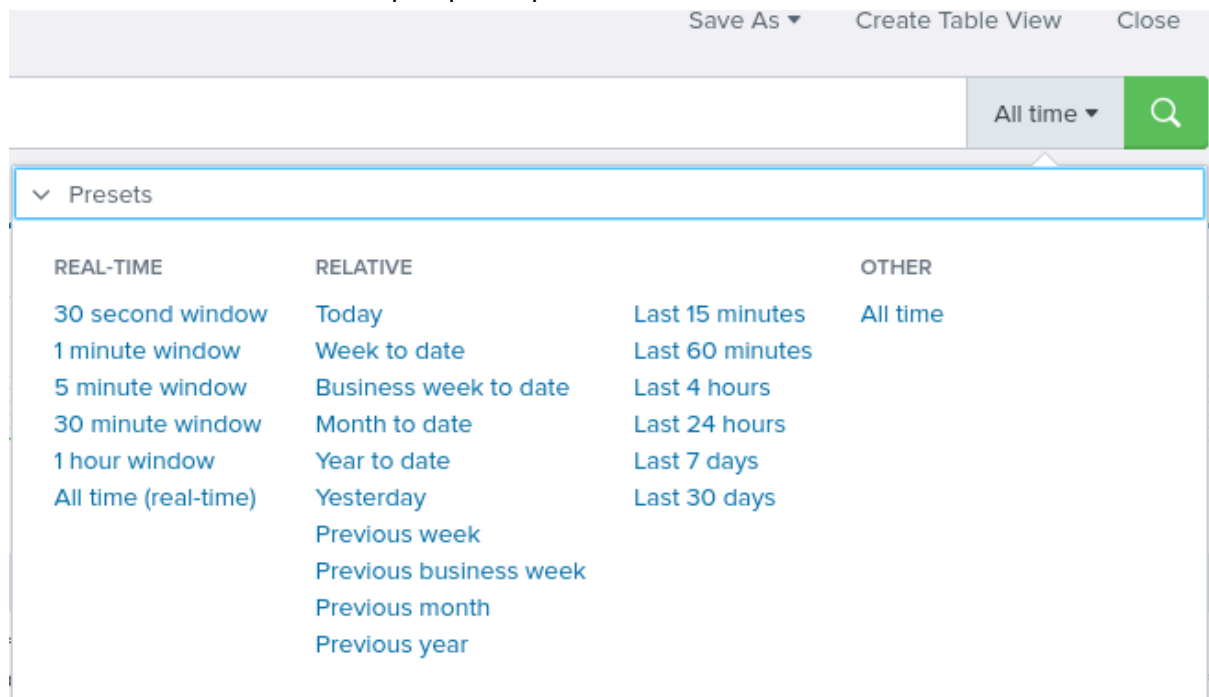


Figura 2 - Configurações do splunk

A própria sala já nos guiou para prestar atenção em logs do suricata, que contém o hostname `imnotreallybatman.com` vindos do IP `40.80.148.42`. A base da nossa query de pesquisa a partir de agora será:

Comando 1: `index=botsv1 imreallynotbatman.com src=40.80.148.42 sourcetype=suricata`

Somente analisando os valores de `dest` já temos alguns valores interessantes que podem indicar um possível ataque de Blind-SQLi. Uma estrutura parecida com a linguagem de SQL e comandos como `sleep()` ou comparações lógicas evidenciam que esse ataque possivelmente foi realizado.

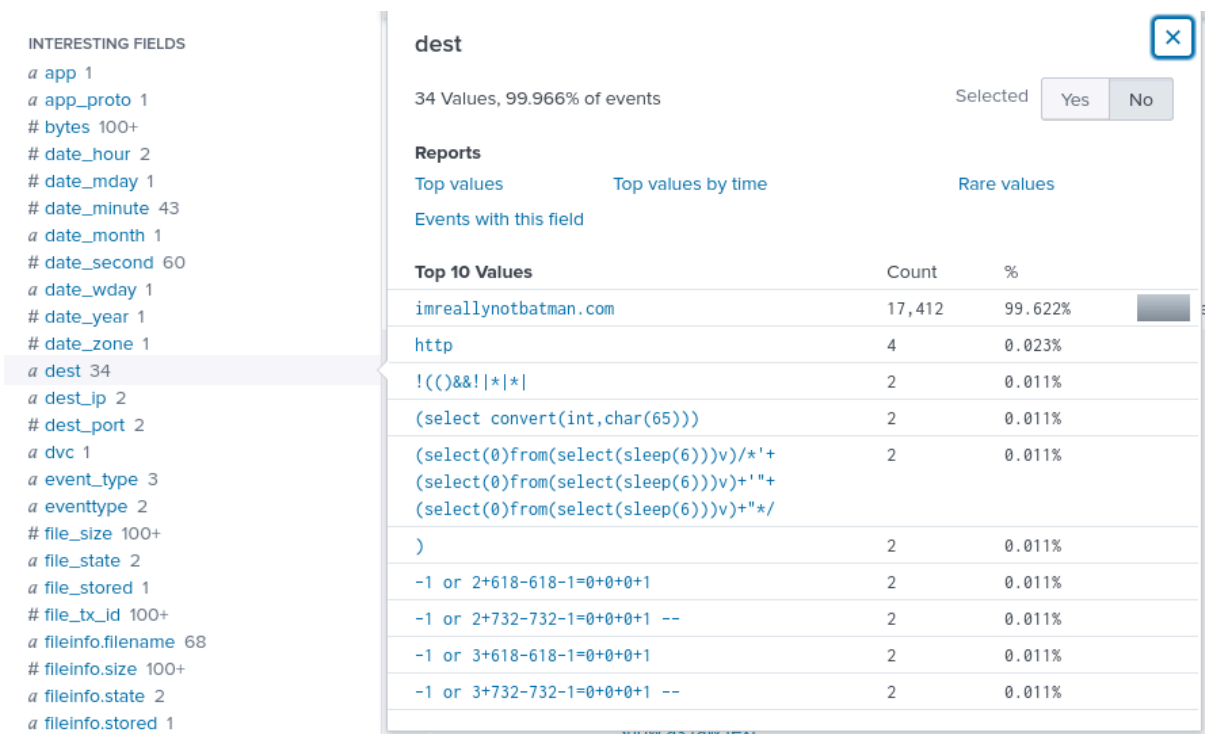


Figura 3 - Resultado do Comando 1.

Um alerta de suricata destacou o valor CVE associado com a tentativa do ataque. Qual é o valor da CVE?

Como estamos procurando o valor da CVE, podemos tentar adicionar o valor CVE a nossa pesquisa:

Comando 2: `index=botsv1 imreallynotbatman.com CVE src_ip=40.80.148.42 sourcetype=suricata`

Event	<input type="checkbox"/> action ▼	allowed	▼
	<input type="checkbox"/> alert.action ▼	allowed	▼
	<input type="checkbox"/> alert.category ▼	Attempted Administrator Privilege Gain	▼
	<input type="checkbox"/> alert.gid ▼	1	▼
	<input type="checkbox"/> alert.rev ▼	1	▼
	<input type="checkbox"/> alert.severity ▼	1	▼
	<input type="checkbox"/> alert.signature ▼	ET WEB_SERVER Possible CVE-2014-6271 Attempt	▼
	<input type="checkbox"/> alert.signature_id ▼	2022028	▼
	<input type="checkbox"/> alert.gid ▼	1	▼
	<input type="checkbox"/> alert_rev ▼	1	▼
	<input type="checkbox"/> bytes ▼	1245	▼
	<input type="checkbox"/> category ▼	Attempted Administrator Privilege Gain	▼

Figura 4 - Resultado do Comando 2.

O CVE-2014-6271 descreve uma vulnerabilidade em que comandos bash podem ser utilizados pelo header. Uma vulnerabilidade diferente da anterior, mas ainda é informação importante para mostrar que vários ataques podem ter sido feitos.

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-6271>

R: CVE-2014-6271

Qual é o CMS que o servidor web usa?

Vamos mudar nosso foco para o servidor Web agora. Mudando nossa pesquisa para filtrar eventos de alerta, podemos ver as diferentes categorias de alerta:

Comando 3: `index=botsv1 imreallynotbatman.com`
`src_ip=40.80.148.42 sourcetype=suricata event_type=alert`

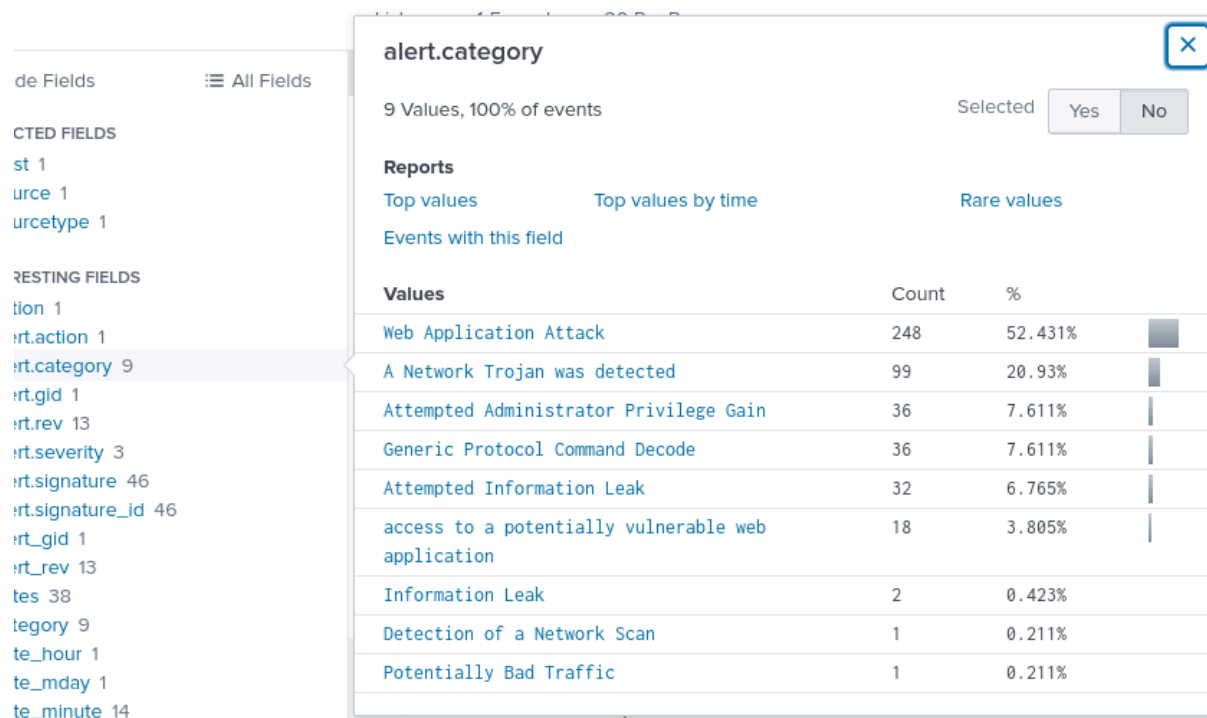


Figura 5 - Resultado do Comando 3.

Já observando o primeiro log, conseguimos achar qual é o CMS analisando somente a URL:

<input type="checkbox"/>	eventtype ▼	suricata_eve_ids_attack (attack ids)	▼
<input type="checkbox"/>	flow_id ▼	2430614826	▼
<input type="checkbox"/>	http.hostname ▼	imreallynotbatman.com	▼
<input type="checkbox"/>	http.http_method ▼	POST	▼
<input type="checkbox"/>	http.http_refer ▼	http://imreallynotbatman.com/joomla/administrator/index.php?option=com_explorer&tmpl=component	▼
<input type="checkbox"/>	http.http_user_agent ▼	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	▼
<input type="checkbox"/>	http.length ▼	0	▼

Figura 6 - Análise da URL nos logs.

R: Joomla

Também vale comentar que na análise dos ataques de aplicação web, conseguimos ver algumas categorias de SQLi, então estávamos certos previamente.

Qual é o web scanner que o atacante utilizou para fazer as tentativas de scan?

Usando o Comando 3 e pesquisando pela categoria “Attempted Information Leak”, conseguimos um log com uma signature bem interessante:

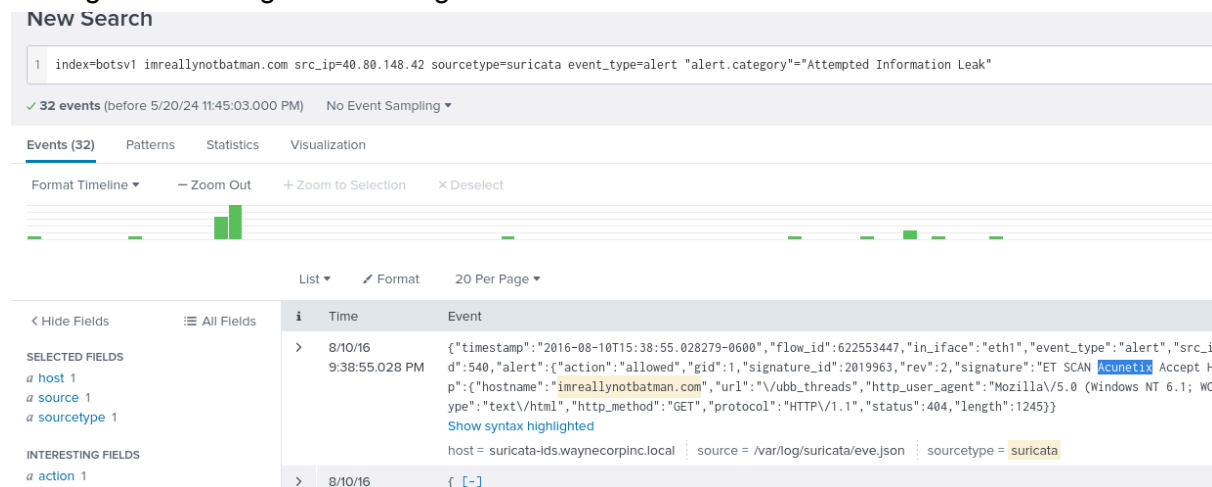


Figura 7 - Logs de alerta de “Attempted Infiltration Leak”.

“ET SCAN Acunetix Accept HTTP Header detected scan in progress”

A frase detected scan chama atenção, e após uma breve pesquisa é possível descobrir que Acunetix é um scanner de vulnerabilidades web.

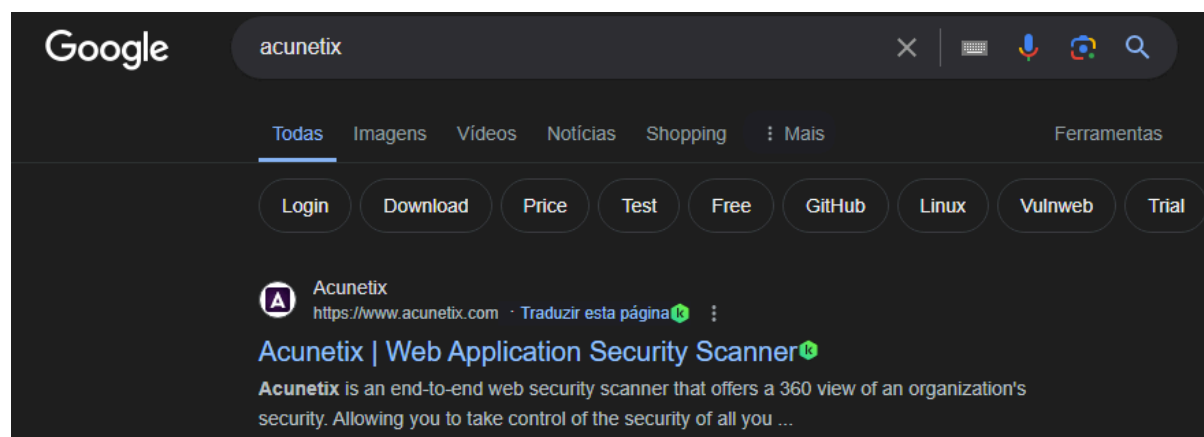


Figura 8 - Pesquisa no google.com para Acutenix.

R: Acunetix

Qual é o endereço de IP do servidor imreallynotbatman.com?

Uma resposta trivial, que pode ser encontrada em qualquer log

```
dest_ip": "192.168.250.70", "
"category": "Attempted Inf
```

Figura 9 - Recorte de um log.

R: 192.168.250.70

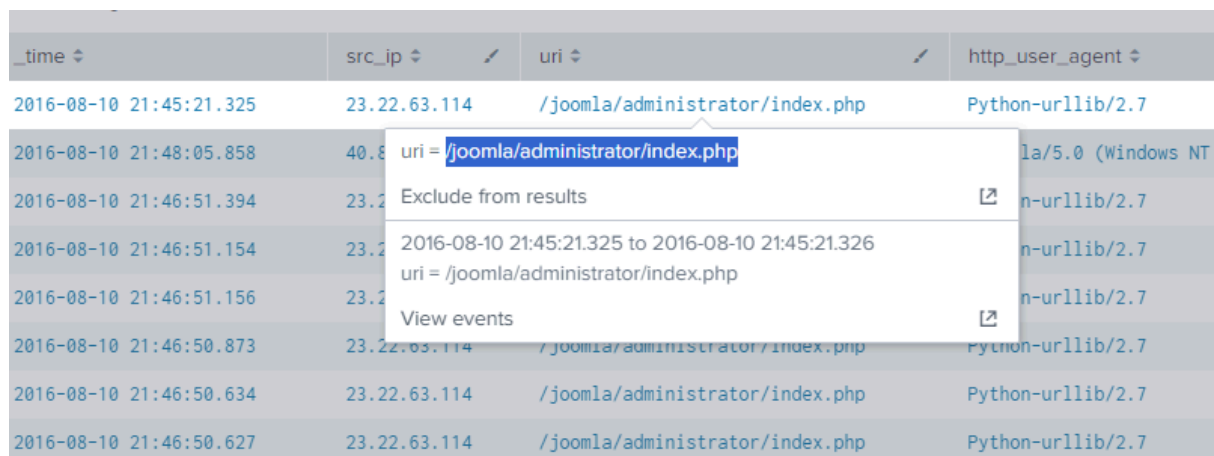
Exploitation Phase

Nesta fase, vamos ver se as tentativas de ataques foram bem sucedidas levando em consideração o IP do atacante identificado na fase anterior. Também devemos levar em consideração que o scanner de vulnerabilidades Acutenix está em uso.

O módulo faz diversas análises estatísticas, explicando seu passo a passo e detalhamento. Para mais detalhes, visite a seção exploitation do módulo. Vamos utilizar o comando final, que já está filtrando senhas e o agente do usuário na página de login administrador do site.

```
Comando 4: index=botsv1 sourcetype=stream:http
dest_ip="192.168.250.70" http_method=POST
form_data=*username*passwd* | rex field=form_data
"passwd=(?<creds>\w+)" | table _time src_ip uri http_user_agent
creds
```

Qual o URI que recebeu múltiplas tentativas de login?



_time	src_ip	uri	http_user_agent
2016-08-10 21:45:21.325	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7
2016-08-10 21:48:05.858	40.82.178.114	/joomla/administrator/index.php	la/5.0 (Windows NT
2016-08-10 21:46:51.394	23.22.63.114	/joomla/administrator/index.php	n-urllib/2.7
2016-08-10 21:46:51.154	23.22.63.114	/joomla/administrator/index.php	n-urllib/2.7
2016-08-10 21:46:51.156	23.22.63.114	/joomla/administrator/index.php	n-urllib/2.7
2016-08-10 21:46:50.873	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7
2016-08-10 21:46:50.634	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7
2016-08-10 21:46:50.627	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7

Figura 10 - Resultado do Comando 4.

R: /joomla/administrator/index.php

Contra qual usuário as tentativas de login foram feitas?

```
Comando 5: index=botsv1 sourcetype=stream:http
dest_ip="192.168.250.70" http_method=POST
uri="/joomla/administrator/index.php"
form_data=*username*passwd* | table _time uri src_ip dest_ip
form_data
```

uri ↕	src_ip ↕	dest_ip ↕	form_data ↕
/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=log
/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=log
/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&d9477575
/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&7ec95c63
/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=log
/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=log

Figura 11 - Resultado do Comando 5.

R: admin

Qual foi a senha correta para o acesso administrador?

Podemos assumir que a senha correta foi a única senha que foi usada duas vezes, uma quando foi encontrada pelo programa, e uma pelo usuário tentando o bruteforce. Para isso, vamos fazer uma contagem de quantas vezes cada valor de senha foi inserido com o seguinte comando:

```
Comando 6: index=botsv1 sourcetype=stream:http
dest_ip="192.168.250.70" http_method=POST
form_data=*username*passwd* | rex field=form_data
"passwd=(?<creds>\w+)" | table src_ip creds | stats count by
creds
```

creds ↕	count ▼
batman	2
000000	1
1111	1
111111	1
11111111	1
112233	1

Figura 12 - Resultado do Comando 6.

R: batman

Quantas senhas únicas foram tentadas?

Investigando os fóruns do Splunk, encontramos que a função `stats dc(variável)` pode contar a quantidade de valores únicos encontrados. Então, modificando o comando 4:

```
Comando 7: index=botsv1 sourcetype=stream:http
dest_ip="192.168.250.70" http_method=POST
form_data=*username*passwd* | rex field=form_data
"passwd=(?<creds>\w+)" | table creds
| stats dc(creds)
```



Figura 13 - Resultado do Comando 7.

R: 412

Qual endereço de IP provavelmente está tentando um ataque de força bruta no host?

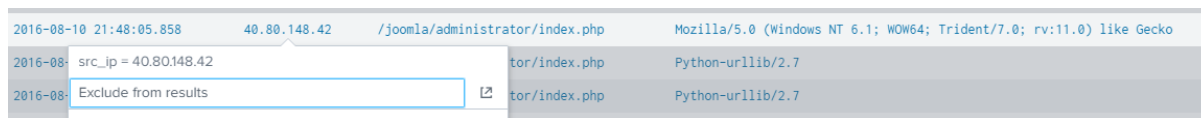
Observando o output do Comando 4, podemos deduzir que o host que está usando python como user agent é o IP que está utilizando um programa de bruteforce.

Observando a Figura X, esse IP é 23.22.63.114

R: 23.22.63.114

Após encontrar a resposta correta, qual IP o atacante usou para acessar e fazer login no painel de administrador?

Utilizando a mesma lógica do exercício anterior, o único IP que realizou login por um agente que não é o python seria o correto.



A screenshot of a Splunk search result table. The table has four columns: Time, IP, URL, and User-Agent. The first row shows a login attempt from IP 40.80.148.42 at 2016-08-10 21:48:05.858 to /joomla/administrator/index.php using Mozilla/5.0. The second and third rows show the same IP and URL but with a Python-urllib/2.7 user-agent. A search bar at the top contains 'src_ip = 40.80.148.42' and a button 'Exclude from results'.

Time	IP	URL	User-Agent
2016-08-10 21:48:05.858	40.80.148.42	/joomla/administrator/index.php	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
2016-08-	src_ip = 40.80.148.42	tor/index.php	Python-urllib/2.7
2016-08-	Exclude from results	tor/index.php	Python-urllib/2.7

Figura 14 - Recorte dos resultados do Comando 5.

R: 40.80.148.42

Installation Phase

Quando o atacante conseguiu passar da segurança e entrou no sistema, ele vai tentar utilizar alguma forma de persistência, seja backdoor ou algum outro aplicativo. Essa é a

fase de instalação. Na última fase, descobrimos que por meio de um ataque de força bruta o atacante conseguiu entrar na página de administrador. Agora é nosso trabalho examinar qual payload foi utilizado para manter a persistência.

O desenvolvimento da sala nos levou a achar que o aplicativo para persistência é “3791.exe”, para mais detalhes sobre a descoberta consulte a sala. Também nos foi dada a query relevante para utilizarmos:

Comando 8: `index=botsv1 "3791.exe" sourcetype="XmlWinEventLog" EventCode=1`

Estamos procurando o 3791.exe nos event logs do windows. Esse comando servirá de base para os próximos desenvolvimentos.

Sysmon também coleta os valores hash dos processos criados. Qual o MD5 do programa 3791.exe?

```
> 8/10/16 9:56:18.000 PM <Event xmlns='http://schemas.microsoft.com/win/2004/8/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFB09}'></Provider><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><OpCode>0</OpCode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-10T21:56:18.14261700Z'></TimeCreated><EventRecordID>428908</EventRecordID><Correlation></Correlation><Execution ProcessID='1296' ThreadID='1416'></Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we1149srv.waynecorpinc.local</Computer><Security UserID='S-1-5-18'></Security><EventData><Data Name='UtcTime'>2016-08-10 21:56:18.142</Data><Data Name='ProcessGuid'>{E500B0EA-A302-57AB-0000-00108D65C301}</Data><Data Name='ProcessId'>3880</Data><Data Name='Image'>C:\inetpub\wwwroot\joomla\3791.exe</Data><Data Name='CommandLine'>3791.exe</Data><Data Name='CurrentDirectory'>C:\inetpub\wwwroot\joomla</Data><Data Name='User'>NT AUTHORITY\IUSR</Data><Data Name='LogonGuid'>{E500B0EA-219E-57AA-0000-0020E3030800}</Data><Data Name='LogonId'>0x3e3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=65DF73D7324D088C83C3E57B445DF0FD43A3A51_MD5=AAE3F5A29935E6ABCC2C2754D12A9AF0_SHA256=EC78C93808453739CA2A37089C275971EC46CAF6E479DE2B2D04E97CC47FA45D_IMPHASH=481F470B82C9C21E108D65F52B04C448</Data><Data Name='ParentProcessId'>2896</Data><Data Name='ParentImage'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='ParentCommandLine'>cmd.exe /c "3791.exe &gt;&gt;1"</Data></EventData></Event>
host = we1149srv | source = WinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwinventlog
```

Figura 15 - Resultado do Comando 8.

R: AAE3F5A29935E6ABCC2C2754D12A9AF0

Olhando os logs, qual usuário executou o programa 3791.exe no servidor?

5-18'>	
<input type="checkbox"/> Task ▾	1
<input type="checkbox"/> TerminalSessionId ▾	0
<input type="checkbox"/> ThreadID ▾	'1416'
<input type="checkbox"/> User ▾	NT AUTHORITY\IUSR
<input type="checkbox"/> UserID ▾	'S-1-5-18'
<input type="checkbox"/> UtcTime ▾	2016-08-10 21:56:18.142
<input type="checkbox"/> Version ▾	5
<input type="checkbox"/> dvc ▾	we1149srv.waynecorpinc.local
<input type="checkbox"/> dvc_nt_host ▾	we1149srv

Figura 16 - Recorte de logs do Comando 8.

R: NT AUTHORITY\IUSR

Procure o hash no VirusTotal. Qual outro nome é associado ao arquivo 3791.exe?

<https://www.virustotal.com/gui/file/ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d/relations>

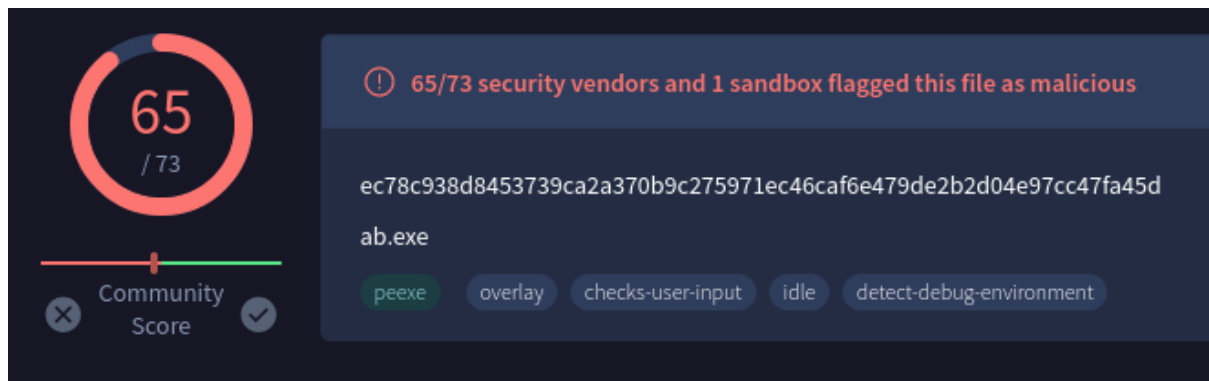


Figura 17 - Pesquisa no VirusTotal.

R: ab.exe

Action on Objective

Como o site sofreu um deface pelo adversário, o ideal seria compreender o que aconteceu no site que causou seu deface. Com a investigação, descobrir que pelo IP 23.22.63.114, o mesmo do bruteforce, o atacante fez download de um arquivo que provavelmente causou o deface.

Comando 9: `index=botsv1`

`url="/poisonivy-is-coming-for-you-batman.jpeg"`

`dest_ip="192.168.250.70" | table _time src dest_ip`

`http.hostname url`

Qual o nome do arquivo que realizou o deface no site?

R: poisonivy-is-coming-for-you-batman.jpeg

O Firewall Fortigate "fortigate_utm" detectou tentativas SQL do IP do atacante 40.80.148.42. Qual o nome da regra que foi ativada durante a tentativa de SQLi?

Comando 10: `index=botsv1 dest_ip="192.168.250.70"`

`sourcetype=fortigate_utm`

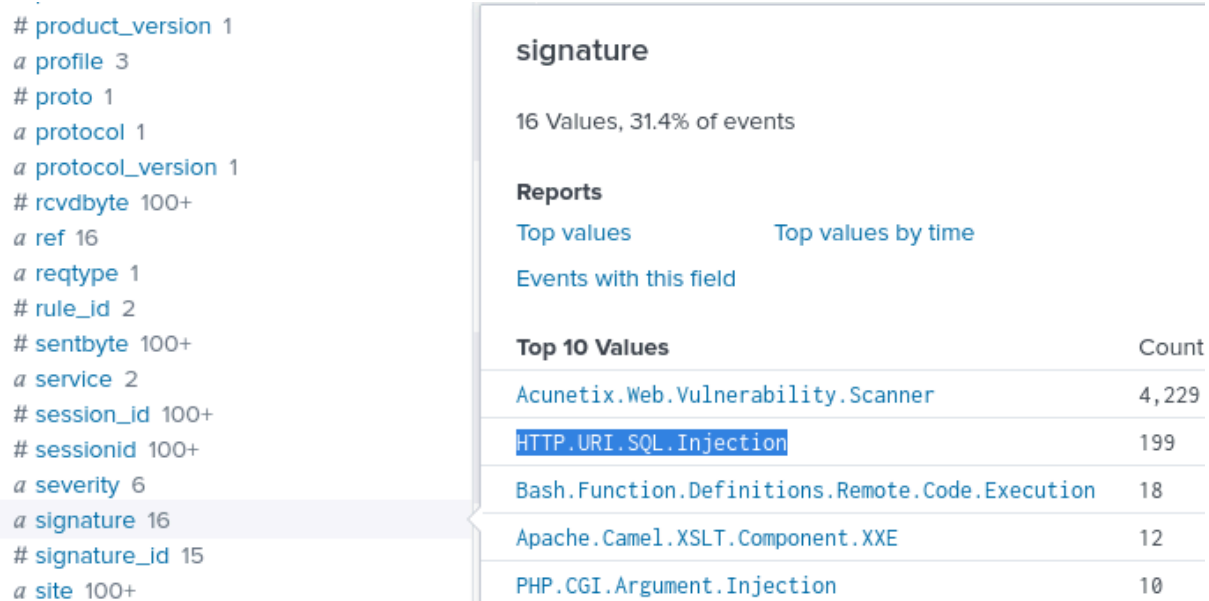


Figura 18 - Resultado do Comando 10.

R: HTTP.URI.SQL.Injection

Command and Control Phase

O atacante fez o upload de um arquivo para o servidor antes de realizar o deface. Para isso, ele fez com que o servidor se conecta-se com um servidor malicioso hospedado pelo adversário, e usou DNS Dinâmico para resolver seu endereço. Nosso objetivo é encontrar o IP que o atacante usou para DNS.

Comando 11: `index=botsv1 sourcetype=stream:http
dest_ip=23.22.63.114 "poisonivy-is-coming-for-you-batman.jpeg"
src_ip=192.168.250.70`

Esse ataque fez uso de DNS dinâmico para resolver o IP malicioso. Qual o nome do domínio qualificado completo associado ao ataque?

```
server_ip: 32337
server_rtt_packets: 2
server_rtt_sum: 64714
site: prankglassinebracket.jumpingcrab.com:1337
src_headers: GET /poisonivy-is-coming-for-you-batman.jpeg |
Host: prankglassinebracket.jumpingcrab.com:1337

src_ip: 192.168.250.70
```

Figura 19 - Resultado do Comando 11.

R: `prankglassinebracket.jumpingcrab.com`

Weaponization Phase

Descobrimos domínios e IPs relacionados ao adversário durante a nossa investigação. Agora, usaremos OSINT para tentar extrair mais informações. Sites usados:

<https://whois.domaintools.com/po1s0n1vy.com>
<https://www.virustotal.com/gui/domain/www.po1s0n1vy.com/relations>
<https://www.robtex.com/ip-lookup/23.22.63.114>

Qual endereço de IP P01s0n1vy atrelou a domínios pré-programados para atacar a Wayne Enterprises?

Date resolved	Detections	Resolver	IP
2024-02-17	0 / 93	VirusTotal	38.207.236.88
2024-01-29	0 / 93	VirusTotal	156.254.170.147
2023-05-25	0 / 93	VirusTotal	172.67.187.244
2023-05-25	0 / 93	VirusTotal	104.21.7.173
2021-09-03	3 / 93	VirusTotal	34.102.136.180
2018-08-30	3 / 93	VirusTotal	91.195.240.117
2018-05-19	0 / 93	VirusTotal	23.22.63.114

Siblings (5)

ftp.po1s0n1vy.com	0 / 93	64.29.151.221			
illian.po1s0n1vy.com	0 / 93	64.29.151.221			
lillian.po1s0n1vy.com	0 / 93	64.29.151.221			
po1s0n1vy.com	0 / 93	52.213.114.86	38.207.236.88	156.254.170.147	...

Figura 20 - Pesquisa no VirusTotal.

O endereço de IP na Figura X está atrelado ao domínio P01s0n1vy e bate com o IP que estava realizando o brute force previamente.

R: 23.22.63.114

Baseado nos dados adquiridos do ataque e fontes de OSINT comuns, qual endereço de email provavelmente está atrelado ao grupo P01s0n1vy?

Usando o site alienvault para procurar sobre o domínio suspeito
<https://otx.alienvault.com/indicator/hostname/www.po1s0n1vy.com>

RECORD ▾	VALUE ▾
Domain Name	POISONIVY.COM
Emails	lillian.rose@po1s0n1vy.com
Emails	hostmaster@retsigler.com
Expiration Date	2017-07-21T00:00:00
Expiration Date	2017-07-21T18:07:13
Name Servers	NS7.ARA.COM

Figura 21 - Pesquisa no Alienvault.

Conseguimos ver que o email atrelado ao domínio é lillian.rose@po1s0n1vy.com

R: lillian.rose@po1s0n1vy.com

Delivery Phase

Agora que identificamos endereços de IP, domínios e emails relacionados ao adversário, nosso objetivo é usar essa informação em plataformas de threat hunting e OSINT para achar mais malware relacionado ao adversário.

<https://www.threatminer.org/host.php?q=23.22.63.114#gsc.tab=0&gsc.q=23.22.63.114&gsc.page=1>

<https://www.virustotal.com/gui/file/9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8>

<https://www.hybrid-analysis.com/sample/9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8?environmentId=100>

Qual é o HASH do malware associado ao grupo APT?

Olhando nossa fonte no threat miner:

Copy

Excel

CSV

PDF

MD5	Detections	
39eecefa9a13293a93bb20036eaf1f5e	N/A	
aae3f5a29935e6abcc2c2754d12a9af0	N/A	
c99131e0169171935c5ac32615ed6261	ALYac	Trojan.GenericKD.3470547
	AVG	Agent5.APHV
	AVware	Trojan.Win32.Generic!BT
	Ad-Aware	Trojan.GenericKD.3470547
	AegisLab	Agent5.Aphv.Gen!c
	AhnLab-V3	Malware/Gen.Generic.N2081883700
	Antiy-AVL	Trojan[Backdoor]/Win32.Redsip
	Arcabit	Trojan.Generic.D34F4D3
	Avira	TR/AD.Zupdax.qmyx

Figura 22 - Pesquisa no Threat Miner.

R: c99131e0169171935c5ac32615ed6261

Qual o nome do malware associado a infraestrutura Poison Ivy?

Checando nossa fonte no VirusTotal:

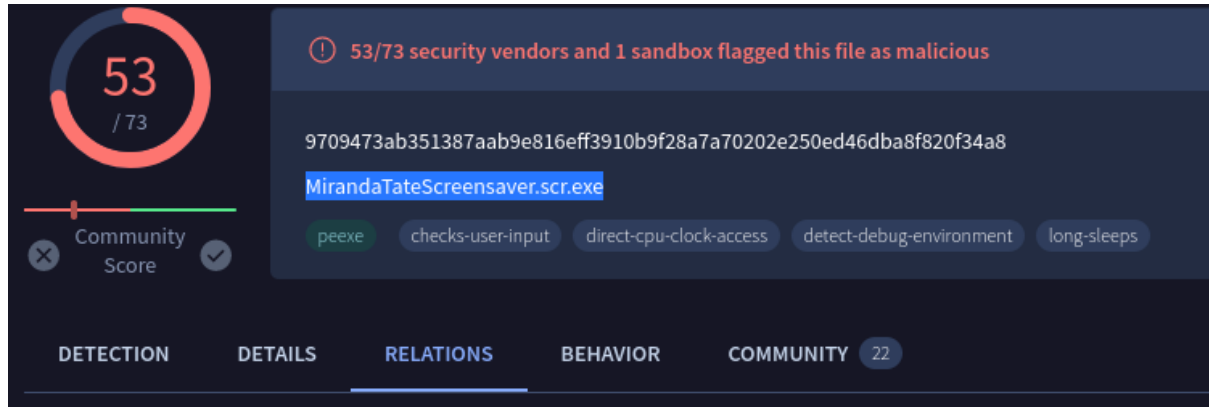


Figura 23 - Segunda pesquisa no VirusTotal.

R: MirandaTateScreensaver.scr.exe