

TRATAMENTO DE INCIDENTES



Paulo Sizino

Analista de segurança da informação -
Accenture (Morphus)



AGENDA

- O que é um incidente?
 - Caso de uso 1
 - Caso de uso 2

5W2H

é um conjunto de questões utilizado para **compor planos de ação** de maneira rápida e eficiente.

- **What:** o que aconteceu?
- **Why:** por que aconteceu? (importante entender o motivo que gerou o incidente)
- **Who:** quem realizou?
- **Where:** onde ocorreu? Que ferramenta?
- **When:** quando realizou?
- **How:** como foi o ocorrido?
- **How much:** qual o impacto/quanto custa? (Essa pergunta busca entender qual é o custo envolvido na realização das tarefas e o custo que o incidente pode causar.)



CASO DE USO 1

Incidente cibernético em andamento

Em um incidente cibernético, tudo inicia com um alerta ou com o ambiente comprometido.

01 – Alerta foi Gerado por causa de uma execução do mimikatz em um servidor;

02 – Ticket Gerado, senso de urgência acionado pelo time de triage e cliente acionado rápido;

03 – Iniciar as análise;

(SIEM): - SEP - Possível atividade de malware não bloqueada Aberto chamad... X

LOG SOURCE INFORMATION: Symantec Endpoint, Syslog - Symantec Endpoint Server

DIRECTION: Unknown
CLASSIFICATION: Malware
COMMON EVENT: Detected Virus Activity
HOST (IMPACTED):
MPE RULE NAME: Virus Found : Left Alone
ZONE (ORIGIN): Unknown
ZONE (IMPACTED): Internal
ENTITY (ORIGIN):
ENTITY (IMPACTED):
USER (IMPACTED): dguard
DOMAIN IMPACTED: Default
OBJECT: Malware
SENDER: gentilkiwi (Benjamin DELPY)
SUBJECT: Hacktool.MimikatzIg4, Infostealerlim
VENDOR MESSAGE ID: Auto-Protect scan
GROUP: My Company\Servidores
SESSION: Heuristic Virus, Virus
PROCESS NAME: mimikatz, mimilove.exe
SEVERITY: info
ACTION: Left alone
VERSION: 2.2.0.0
COMMAND: Left alone
OBJECT NAME: 31EB1DE7E840A342FD468E558E5AB627BCB4C542A8FE01AEC4D5BA01D539A0FC,
B42725211240828CC505D193D8EA5915E395C9F43E71496FF0ECE4F72E3E4AB
STATUS: Reputation was not used in this detection
THREAT NAME: Hacktool.MimikatzIg4, Infostealerlim

LOG MESSAGES

12 06 2021 12:45:03 <LPTR:INFO> Dec 6 12:45:03 Virus found, IP Address:
Computer name: , Source: Auto-Protect scan, Risk name: Hacktool.MimikatzIg4, Occurrences: 1, File path:
C:\Users\dguard\Music\mimikatz New\x64\mimikatz.exe, Description: Actual action: Left alone, Requested action: Left alone, Secondary action:
Left alone, Event time: 2021-12-06 12:43:15, Event Insert Time: 2021-12-06 12:45:03, End Time: 2021-12-06 12:43:16, Last update time: 2021-12-06
12:45:03, Domain Name: Default, Group Name: My Company\Servidores, Server Name: , User Name:
dguard, Source Computer Name: , Source Computer IP: , Disposition: Reputation was not used in this detection, Download site: , Web domain:
Downloaded by: c:/windows/explorer.exe, Prevalence: Reputation was not used in this detection, Confidence: Reputation was not used in this
detection, URL Tracking Status: On, First Seen: Reputation was not used in this detec

O Que podemos ver no alerta?

Quando ocorreu?

R: 12/06/21 as 12:45

Quem executou?

R: usuario "dguard"

Qual o servidor?

R: server01

Qual o arquivo e hash?

R: "mimikatz.exe" e
"mimilove.exe"

•31EB1DE7E840A342FD468E558
E5AB627BCB4C542A8FE01AEC4
D5BA01D539A0FC

•B42725211240828CCC505D193
D8EA5915E395C9F43E71496FF0
ECE4F72E3E4AB

(SIEM): - SEP - Possível atividade de malware não bloqueada

Aberto chamad... X

LOG SOURCE INFORMATION: Symantec Endpoint, Syslog - Symantec Endpoint Server)

DIRECTION: Unknown

CLASSIFICATION: Malware

COMMON EVENT: Detected Virus Activity

HOST (IMPACTED): server01

MPE RULE NAME: Virus Found : Left Alone

ZONE (ORIGIN): Unknown

ZONE (IMPACTED): Internal

ENTITY (ORIGIN):

ENTITY (IMPACTED):

USER (IMPACTED): dguard

DOMAIN IMPACTED: Default

OBJECT: Malware

SENDER: gentilkiwi (Benjamin DELPY)

SUBJECT: Hacktool.Mimikatz!g4, Infostealer!im

VENDOR MESSAGE ID: Auto-Protect scan

GROUP: My Company\Servidores

SESSION: Heuristic Virus, Virus

PROCESS NAME: mimikatz, mimilove.exe

SEVERITY: info

ACTION: Left alone

VERSION: 2.2.0.0

COMMAND: Left alone

OBJECT NAME: 31EB1DE7E840A342FD468E558E5AB627BCB4C542A8FE01AEC4D5BA01D539A0FC, B42725211240828CCC505D193D8EA5915E395C9F43E71496FF0ECE4F72E3E4AB

STATUS: Reputation was not used in this detection

THREAT NAME: Hacktool.Mimikatz!g4, Infostealer!im

LOG MESSAGES

12 06 2021 12:45:03 <LPTR:INFO> Dec 6 12:45:03 Virus found, IP Address: , Computer name: , Source: Auto-Protect scan, Risk name: Hacktool.Mimikatz!g4, Occurrences: 1, File path: C:\Users\dguard\Music\mimikatz New\x64\mimikatz.exe, Description: Actual action: Left alone, Requested action: Left alone, Secondary action: Left alone, Event time: 2021-12-06 12:43:15, Event Insert Time: 2021-12-06 12:45:03, End Time: 2021-12-06 12:43:16, Last update time: 2021-12-06 12:45:03, Domain Name: Default, Group Name: My Company\Servidores, Server Name: , User Name: dguard, Source Computer Name: , Source Computer IP: , Disposition: Reputation was not used in this detection, Download site: , Web domain: , Downloaded by: c:/windows/explorer.exe, Prevalence: Reputation was not used in this detection, Confidence: Reputation was not used in this detection, URL Tracking Status: On, First Seen: Reputation was not used in this detec

Quais ações recomendadas?

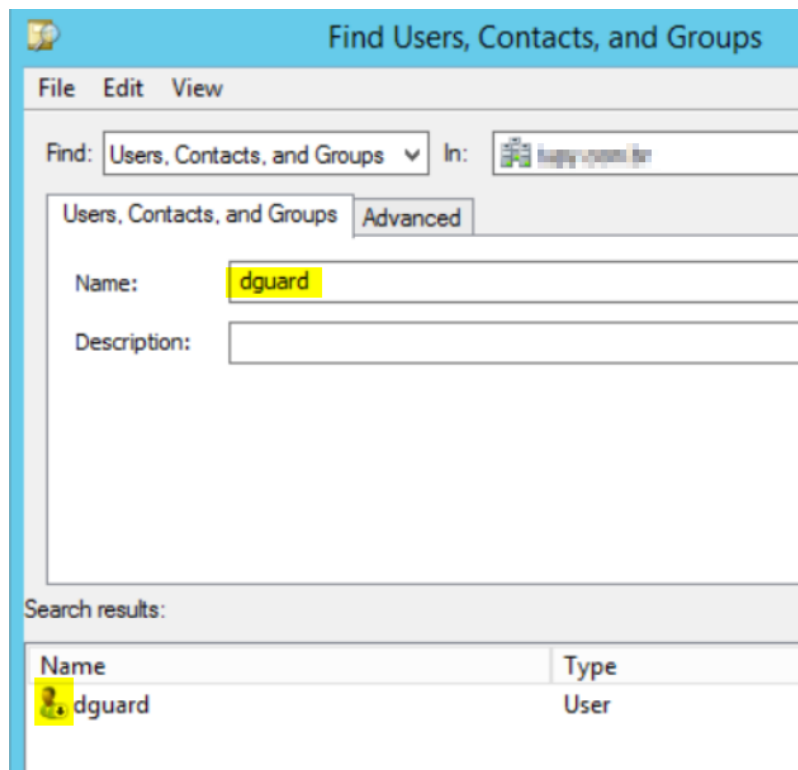
Contenção

- Bloqueio de hashes e artefatos;
- Bloqueio do usuário.

Análise

- Quais permissões do usuário?
- Qual utilidade do usuário?
- Hunting via SIEM das ações do usuário.
- Analise do servidor :
 - Usuário ainda logado?
 - Processos que estão em execução?
 - Conexões que o computador mantém aberta?

Bloqueio do usuário



Hunting via SIEM

Host (Impacted)	User (Impacted)	Process Name	Subject
server03	dguard	mimikatz.exe	hacktool.mimikatz
server03	dguard	mimidrv (mimikatz)	hacktool.mimikatz
server02	dguard	mimilove.exe	infostealer!im
server02	dguard	mimikatz	hacktool.mimikatz
server02	dguard	mimilove.exe	infostealer!im
server01	dguard	mimilove.exe	infostealer!im
server01	dguard	mimikatz	hacktool.mimikatz
server01	dguard	mimikatz	hacktool.mimikatz

Análise do ambiente

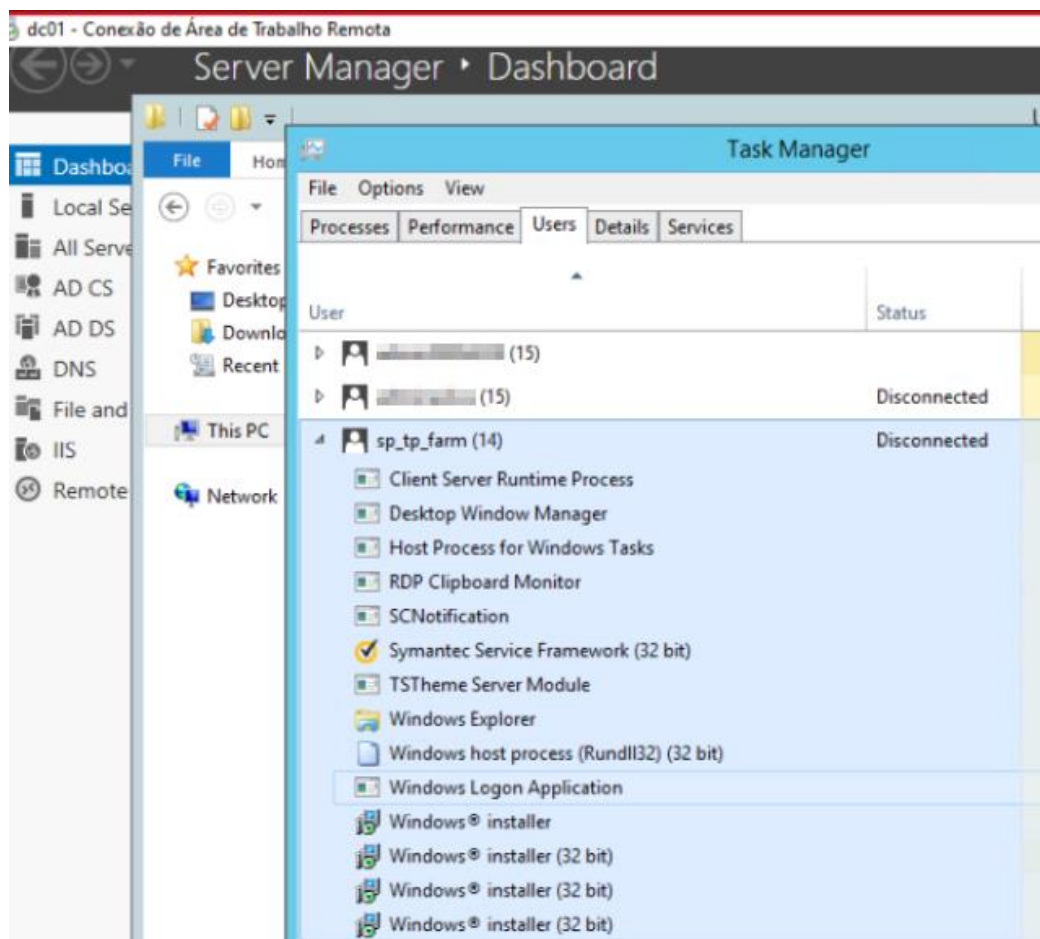
Domain Controlers

- Uma pratica é já analisar como está a saúde dos principais hosts do ambiente como pro exemplo domain controlers, servidores de Exchange, file servers e hosts da DMZ.

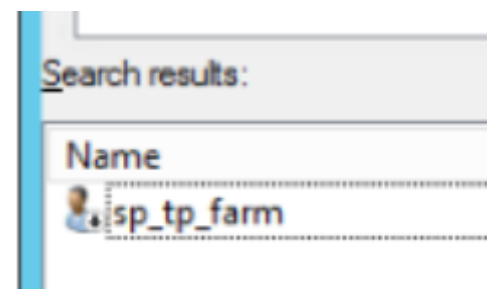
O que analisar?

- Acesso remoto (interativo) RDP, SSH, FTP entre outras;
- Criação de usuários não mapeados;
- Hosts com saída para internet;
- Habilitação de usuários;
- Tarefas agendadas;
- Comandos suspeitos (4688 e 4104)

Analise do DC



Para nossa surpresa, ao acessar o Domain Controller, identificamos uma conta de serviço conectada chama “SP_TP_FARM” e de imediato já solicitamos o bloqueio da conta.



Foi solicitado também o resete de senha dos outros 2 usuários conectados no host, para prevenir que eles fossem utilizados pelo atacante.

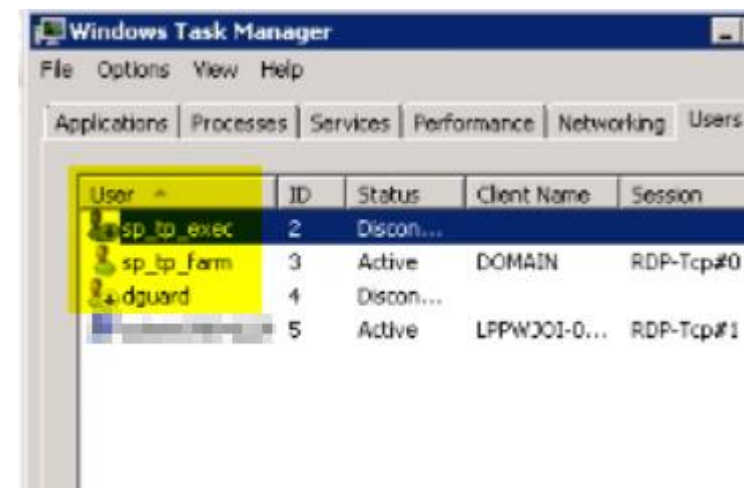
Analise do incidente

Após análise do usuário via SIEM, foi identificado que o acesso remoto "Event ID 4624 Tipo 10" teve origem o host:

"Mex01 (10.4.1.82)"

Até então este servidor era desconhecido pelo nosso time, não existia no SIEM e o time do cliente somente sabia dizer "não conheço"

Decidimos então ir ao servidor para realizar uma análise e para nossa surpresa, lá estava o usuário "**dguard**" que gerou o primeiro alerta, o usuário "**sp tp farm**" e um novo usuário "**sp tp exec**".



Analise de conexões ativas!

Abrindo o CMD, rodamos o comando **"Netstat -n | find \"ESTA\"** identificamos conexões **ATIVAS** com a porta **3389**.

Chegamos ao **\"Vetor inicial\"**, após analisar todos os logs do servidor Mex01, identificamos um brute force no RDP que estava exposto a internet e a partir daí o atacante conseguiu acesso e pivotar para outras redes!

```
C:\Users\>netstat -n | find "ESTA"
```

TCP	0.0.0.0:80	10.4.8.40:55707	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.40:55708	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.40:55709	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.184:54979	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.184:54980	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.184:54981	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.184:54982	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.184:54983	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.184:54984	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.194:50935	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.194:50937	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.8.194:50938	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.9.30:50100	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.9.51:54675	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.9.51:54676	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.9.51:54677	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.9.51:54678	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.9.51:54679	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.56:53070	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.56:53081	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.56:53082	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.184:60676	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.184:60682	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.104:60603	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.250:63615	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.250:63616	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.250:63617	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.250:63618	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.250:63619	ESTABLISHED	4
TCP	0.0.0.0:80	10.4.20.250:63620	ESTABLISHED	4
TCP	0.0.0.0:80	10.71.8.50:60721	ESTABLISHED	4
TCP	0.0.0.0:80	10.71.8.50:60722	ESTABLISHED	4
TCP	0.0.0.0:80	10.71.8.50:60723	ESTABLISHED	4
TCP	0.0.0.0:80	10.71.8.50:60724	ESTABLISHED	4
TCP	0.0.0.0:80	10.71.8.50:60725	ESTABLISHED	4
TCP	0.0.0.0:80	10.71.8.50:60726	ESTABLISHED	4
TCP	0.0.0.0:3389	92.246.89.137:53387	ESTABLISHED	3028
TCP	0.0.0.0:3389	157.90.177.188:55450	ESTABLISHED	3028
TCP	0.0.0.0:3389	157.90.177.188:60203	ESTABLISHED	3028
TCP	0.0.0.0:3389	176.97.37.43:61227	ESTABLISHED	3028
TCP	0.0.0.0:3389	192.168.14.96:57870	ESTABLISHED	3028
TCP	0.0.0.0:49499	172.16.100.123:445	ESTABLISHED	1304
TCP	0.0.0.0:49652	10.4.1.127:445	ESTABLISHED	4
TCP	0.0.0.0:50206	10.4.1.127:49159	ESTABLISHED	500
TCP	0.0.0.0:52449	172.16.100.123:445	ESTABLISHED	4
TCP	0.0.0.0:53363	172.16.100.123:445	ESTABLISHED	4
TCP	0.0.0.0:53587	10.4.1.164:55406	ESTABLISHED	2120
TCP	0.0.0.0:53636	10.4.1.164:55406	ESTABLISHED	2120
TCP	0.0.0.0:53646	10.4.1.164:55406	ESTABLISHED	2120
TCP	0.0.0.0:53647	10.4.1.164:55406	ESTABLISHED	2120
TCP	0.0.0.0:53664	10.4.1.164:55406	ESTABLISHED	2120
TCP	0.0.0.0:53673	10.4.1.164:55406	ESTABLISHED	2120
TCP	0.0.0.0:53675	10.4.1.164:55406	ESTABLISHED	2120

Melhorias pós incidente

Quick Wins

- Revisão de regras permissivas e com liberação externa para portas de conexão remota (3389, 22...)
- Adição de novas fontes de logs (visibilidade)
- Revisão de contas de serviços para o SIEM monitorar

Regras

- Acesso RDP via contas de serviços
- Acesso RDP via IP Publico
- Criação de regras permissivas no FW

Auditorias

- Habilitação de eventos de auditoria Powershell e Criação de processos (4104 e 4688)



CASO DE USO 2

Possível Incidente cibernético

Em um incidente cibernético, tudo inicia com um alerta ou com o ambiente comprometido.

01 – Alerta foi Gerado por causa de multiplas autenticações partindo de um servidor;

02 – Usuários não eram do ambiente;

User (Origin) Top 20 by Log Count			
Value	Percent	Log Co	
administrador	22%	6759,0	
administrator	16%	4941,0	
admin	04%	1150,0	
user	03%	826,0	
test	02%	753,0	
usuario	02%	736,0	
server	02%	732,0	
support	02%	732,0	
remote	02%	731,0	
sistemas	02%	731,0	
sistema	02%	730,0	
remoto	02%	729,0	
remota	02%	729,0	
recepccion	02%	729,0	
usuaria	02%	729,0	
caja	02%	728,0	
utilizador	02%	728,0	
servidor	02%	728,0	
prueba	02%	728,0	

[Ticket#2019010101] [-] (SIEM) - AIE: AD - Possivel Password Spray

#ALARME DATE: 2019010101

ALARME ID: 123456

Prezado(a),

Identificamos uma possível atividade para ataque de "Password Spray" partindo do host 10.10.10.10 onde possivelmente a conta afetada é administrator, esta regra:

Identifica um possível evento de "Password Spray" em uma credencial do AD no ambiente do cliente. O password spray é uma modalidade de ataque onde usa-se um refinamento de senhas para tentativas de acesso por força bruta. De maneira mais simples, é uma senha bem-preparada e comum a várias senhas de usuários.

Sugestões de ações:

Defina políticas de bloqueio de conta após um certo número de tentativas de login com falha para impedir que as senhas sejam adivinhadas. Uma política muito rigorosa pode criar uma condição de negação de serviço e tornar os ambientes inutilizáveis, com todas as contas usadas na força bruta sendo bloqueadas.

Use a autenticação multifator. Sempre que possível, habilite também a autenticação multifator em serviços voltados para o exterior.

Consulte as diretrizes do NIST ao criar diretivas de senha.

Monitore muitas tentativas de autenticação com falha em várias contas que podem resultar de tentativas de pulverização de senha. É difícil detectar quando os hashes são quebrados, uma vez que isso geralmente é feito fora do escopo da rede de destino. (por exemplo: Windows EID 4625 ou 5379).

Usar WordBlockList no ambiente (<https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection>).

Utilizar um cofre de senhas, que permite tanto administrar senha como gerar senhas robustas para cada recurso, com base nas regras que o administrador decidir.

O Que podemos ver no alerta?

Quando ocorreu?

R: Mais de 2 dias de alertas

Quem executou?

R: **Usuários que não são do ambiente**

Qual o servidor?

R: **Autenticação tendo origem o próprio AD**

TICKET#	IDADE	REMETENTE	TITULO
2023-01-10-10-10-10	1 d 0 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-11-10-10	1 d 1 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-12-10-10	1 d 2 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-13-10-10	1 d 2 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-14-10-10	1 d 3 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-15-10-10	1 d 5 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-16-10-10	1 d 9 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-17-10-10	1 d 9 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-18-10-10	1 d 13 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-19-10-10	1 d 13 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-20-10-10	1 d 14 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-21-10-10	1 d 14 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-22-10-10	1 d 15 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-23-10-10	1 d 15 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-24-10-10	1 d 16 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-25-10-10	1 d 20 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-26-10-10	1 d 20 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-27-10-10	1 d 21 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-28-10-10	1 d 21 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-29-10-10	2 d 14 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-30-10-10	2 d 17 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-10-31-10-10	2 d 18 h	Segurança da Informação	(SIEM) -AIE: AD - Possível Password Spray
2023-01-11-01-10-10	2 d 19 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-11-02-10-10	2 d 19 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-11-03-10-10	2 d 20 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-11-04-10-10	2 d 21 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-11-05-10-10	2 d 21 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray
2023-01-11-06-10-10	2 d 21 h	AD - Possível Password Spray	(SIEM) -AIE: AD - Possível Password Spray

Quais ações recomendadas? + • ○

Análise

- Analise de logs;
 - Security
 - NetLogon

```
02/28 15:06:30 [LOGON] [8544] GCB: SamLogon: Transitive Network logon of  
(null)\bizmacdev from B_12 (via APPAZU28) Returns 0xc0000064
```

Basic Information	
Normal Date:	terça-feira, 28 de fevereiro de 2023 15:06:31.061
Last Normal Date:	N/A
Log Count:	1,0
Log Source Entity:	
Log Source Host:	SDCAZU02
Log Source:	SDCAZU02 Microsoft Netlogon
Log Source Type:	Flat File - Microsoft Netlogon
Processed Information	
Priority	35,0
Direction/Zone:	Unknown (Unknown -> Internal)
Classification:	Authentication Failure
Common Event:	User Logon Failure : Bad Username
MPE Rule:	User does not exist
Event ID:	204

Processed Meta Data Fields	
Field	Value
Entity (Origin)	
Entity (Impacted)	
HostName (Origin)	b_12
Known Host (Impacted)	APPAZU28
HostName (Impacted)	appazu28
User (Origin)	bizmacdev
Domain Impacted	(null)
Severity	logon

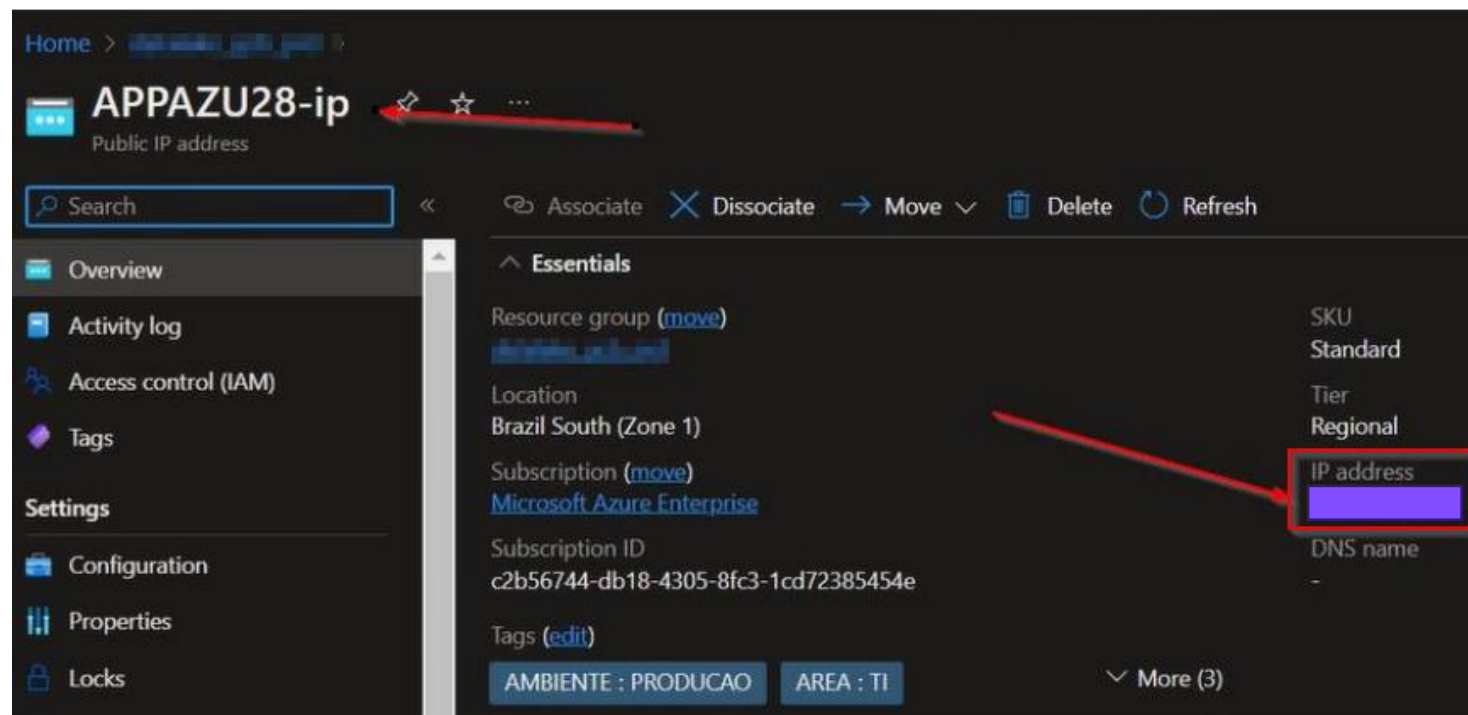
Basic Information	
Normal Date:	quinta-feira, 2 de março de 2023 13:50:22.664
Last Normal Date:	N/A
Log Count:	1,0
Log Source Entity:	
Log Source Host:	APPAZU28
Log Source:	APPAZU28 WinEvtXML - Security
Log Source Type:	MS Windows Event Logging XML - Security
Processed Information	
Priority	35,0
Direction/Zone:	External (External -> Unknown)
Classification:	Authentication Failure
Common Event:	User Logon Failure : Bad Username
MPE Rule:	EVID 4625 : User Logon Type 3: No Such Username
Event ID:	11.135

Processed Meta Data Fields	
Field	Value
Vendor Message ID	4625
Entity (Origin)	Global Entity
Entity (Impacted)	
Location (Origin)	Russia, Omskaja oblast', Omsk
IP Address (Origin)	87.251.64.140
HostName (Origin)	b_11
HostName (Impacted)	appazu28.gcb.local
TCP/UDP Port (Origin)	0
User (Origin)	administrador
Domain Impacted	hg33
Object	0xc000006d
Command	3
Process Name	ntlmssp
Severity	information
Session	0x0
Status	0xc0000064

Identificado que o host estava alocado no Azure (depois de muito tempo o cliente tentando identificar);

Porém, o ambiente do Azure tinha um Fortigate na borda e o cliente jurava de pé junto que não existia publicação do host...

...Mas alguém fez uma configuração diretamente do Host para internet sem passar pelo Fortigate criando um IP PÚBLICO.



Testes realizados para demonstrar que estava com a porta aberta para internet:

- RDP
- NMAP

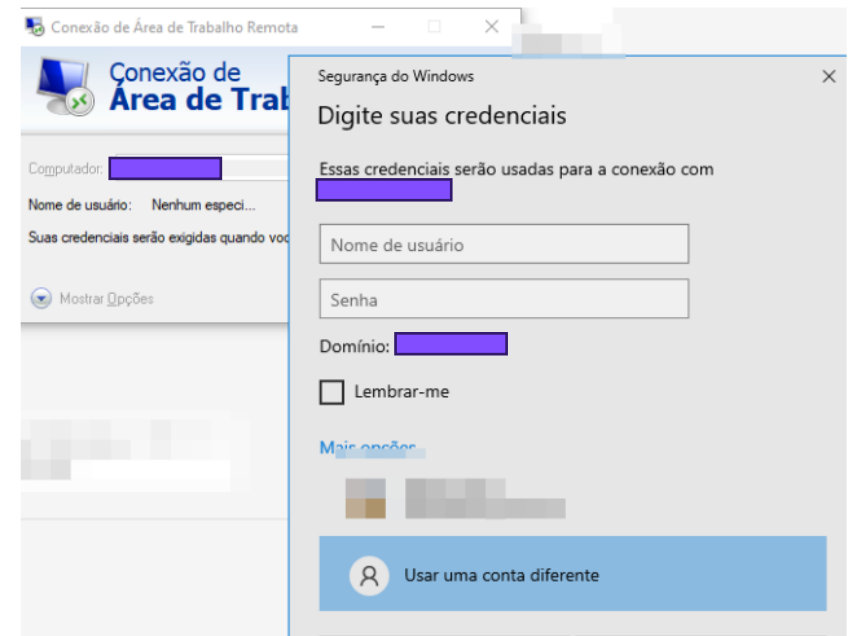
```

$ sudo nmap -v -sV -Pn -n -p3389 [redacted]
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 16:18 -03
NSE: Loaded 45 scripts for scanning.
Initiating SYN Stealth Scan at 16:18
Scanning 191.233.246.50 [1 port]
Discovered open port 3389/tcp on 191.233.246.50
Completed SYN Stealth Scan at 16:18, 0.04s elapsed (1 total ports)
Initiating Service scan at 16:18
Scanning 1 service on 191.233.246.50
Completed Service scan at 16:19, 6.02s elapsed (1 service on 1 host)
NSE: Script scanning 191.233.246.50.
Initiating NSE at 16:19
Completed NSE at 16:19, 0.00s elapsed
Initiating NSE at 16:19
Completed NSE at 16:19, 0.00s elapsed
Nmap scan report for 191.233.246.50
Host is up (0.0050s latency).













PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.57 seconds
Raw packets sent: 1 (44B) | Rcvd: 1 (44B)

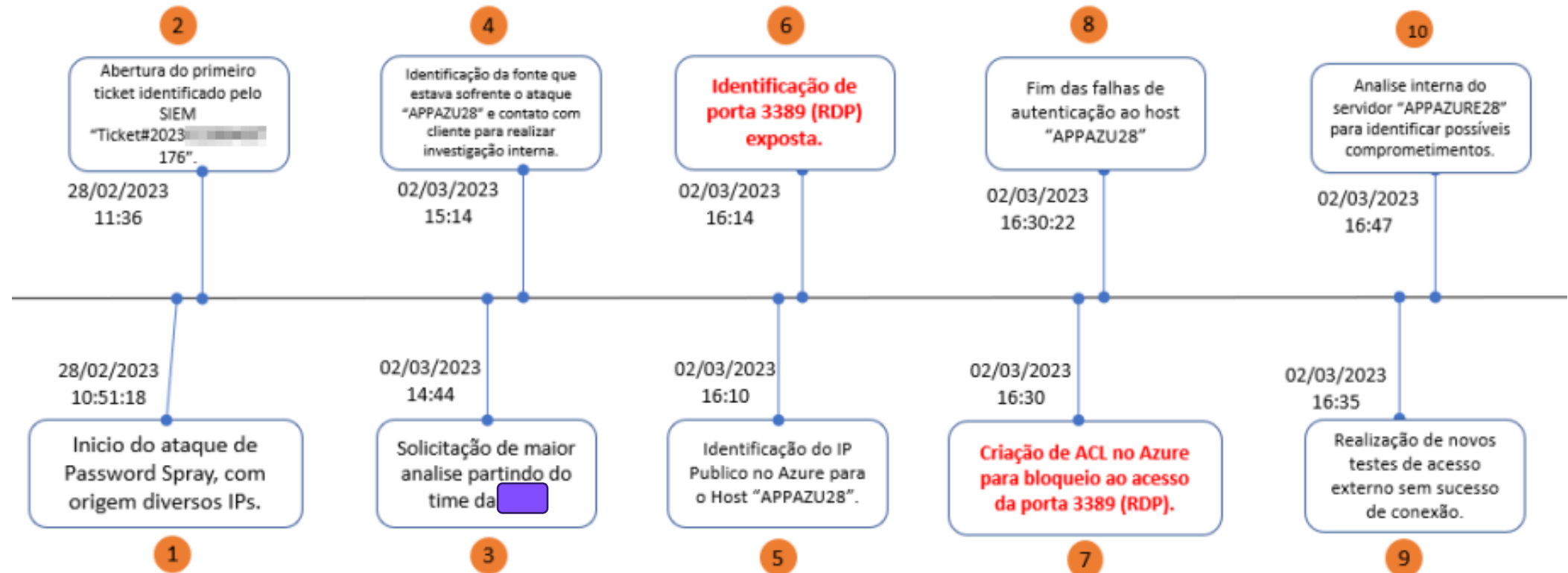
```



Exemplos de Ips que estavam tentando conectar no ambiente.

<p>80.66.88.210 was found in our database!</p> <p>This IP was reported 889 times. Confidence of Abuse is 60%:</p> <div><div>60%</div></div> <table><tr><td>ISP</td><td>Alexander Valerevich Mokhonko</td></tr><tr><td>Usage Type</td><td>Data Center/Web Hosting/Transit</td></tr><tr><td>Domain Name</td><td>serverlux.ru</td></tr><tr><td>Country</td><td> Netherlands</td></tr><tr><td>City</td><td>Amsterdam, Noord-Holland</td></tr></table>	ISP	Alexander Valerevich Mokhonko	Usage Type	Data Center/Web Hosting/Transit	Domain Name	serverlux.ru	Country	 Netherlands	City	Amsterdam, Noord-Holland	<p>80.66.88.207 was found in our database!</p> <p>This IP was reported 775 times. Confidence of Abuse is 56%:</p> <div><div>56%</div></div> <table><tr><td>ISP</td><td>Alexander Valerevich Mokhonko</td></tr><tr><td>Usage Type</td><td>Data Center/Web Hosting/Transit</td></tr><tr><td>Domain Name</td><td>serverlux.ru</td></tr><tr><td>Country</td><td> Netherlands</td></tr><tr><td>City</td><td>Amsterdam, Noord-Holland</td></tr></table>	ISP	Alexander Valerevich Mokhonko	Usage Type	Data Center/Web Hosting/Transit	Domain Name	serverlux.ru	Country	 Netherlands	City	Amsterdam, Noord-Holland
ISP	Alexander Valerevich Mokhonko																				
Usage Type	Data Center/Web Hosting/Transit																				
Domain Name	serverlux.ru																				
Country	 Netherlands																				
City	Amsterdam, Noord-Holland																				
ISP	Alexander Valerevich Mokhonko																				
Usage Type	Data Center/Web Hosting/Transit																				
Domain Name	serverlux.ru																				
Country	 Netherlands																				
City	Amsterdam, Noord-Holland																				
<p>80.66.88.203 was found in our database!</p> <p>This IP was reported 2,590 times. Confidence of Abuse is 53%:</p> <div><div>53%</div></div> <table><tr><td>ISP</td><td>Alexander Valerevich Mokhonko</td></tr><tr><td>Usage Type</td><td>Data Center/Web Hosting/Transit</td></tr><tr><td>Domain Name</td><td>serverlux.ru</td></tr><tr><td>Country</td><td> Netherlands</td></tr><tr><td>City</td><td>Amsterdam, Noord-Holland</td></tr></table>	ISP	Alexander Valerevich Mokhonko	Usage Type	Data Center/Web Hosting/Transit	Domain Name	serverlux.ru	Country	 Netherlands	City	Amsterdam, Noord-Holland	<p>80.66.88.212 was found in our database!</p> <p>This IP was reported 866 times. Confidence of Abuse is 56%:</p> <div><div>56%</div></div> <table><tr><td>ISP</td><td>Alexander Valerevich Mokhonko</td></tr><tr><td>Usage Type</td><td>Data Center/Web Hosting/Transit</td></tr><tr><td>Domain Name</td><td>serverlux.ru</td></tr><tr><td>Country</td><td> Netherlands</td></tr><tr><td>City</td><td>Amsterdam, Noord-Holland</td></tr></table>	ISP	Alexander Valerevich Mokhonko	Usage Type	Data Center/Web Hosting/Transit	Domain Name	serverlux.ru	Country	 Netherlands	City	Amsterdam, Noord-Holland
ISP	Alexander Valerevich Mokhonko																				
Usage Type	Data Center/Web Hosting/Transit																				
Domain Name	serverlux.ru																				
Country	 Netherlands																				
City	Amsterdam, Noord-Holland																				
ISP	Alexander Valerevich Mokhonko																				
Usage Type	Data Center/Web Hosting/Transit																				
Domain Name	serverlux.ru																				
Country	 Netherlands																				
City	Amsterdam, Noord-Holland																				

Cronologia



+



o



.



OBRIGADO

Paulo Sizino
paulosizino@gmail.com