DarkSide Ransomware Operations – Preventions and Detections.

blueteamblog.com/darkside-ransomware-operations-preventions-and-detections

May 14, 2021

By Auth 0r / May 14, 2021 / Cybersecurity, SIEM, Threat Hunting, Threat Intelligence
No Comments

I decided to release this blog post as a longer form, more in depth version of this twitter thread I released on the 12th of May. The aim of this blog post is to provide you with actionable prevention's and detection's against known TTPs which have been seen during DarkSide ransomware operations from the group and their affiliates.

It is important to note that many of these prevention's and detection's will work not only for this group, but for preventing and detecting attacks from many threat actors due to their generic nature.

This thread was in response to the fantastic blog post by FireEye – "Shining a Light on DARKSIDE Ransomware Operations" released on the 10th of May.

Before getting into the post, here are some further reading resources on DarkSide if you are interested.

Time to get into the detection's and prevention's. I have listed a large number of SIEM rules below which I have had stored on a personal database for a while. I can't remember exactly who created each and every one of them (Various people – it wasn't me) – but apologies that I am unable to give particular credits for these. I know some were created by Florian Roth, Samir Bousseaden, Markus Neis and Roberto Rodriguez. I hope however sharing them will make up for this in providing further detection's to the community.

Also, for all the SIEM rules I have listed below, keep sure of three things if you create them. 1. Do you have the correct auditing configured, 2. Are the logs in your SIEM, 3. Are the properties being parsed correctly. If any of these answer no, they won't work.

INITIAL COMPROMISE

Password attacks on perimeter

The first initial compromise method mentioned was password spray attacks against VPNs.

This is extremely common, but luckily for us relatively easy to protect against compared to other attack vectors. Password spray attacks and brute forces will happen not just against VPN's but any public facing authentication methods, such as Azure Active Directory.

I know everyone says this, but they say it for a reason – Multi-factor authentication should be used for all accounts in your network. Also ensure users are using unique passwords for each service / platform they have access too. This will make the likelihood of a password attack breaching your perimeter a lot lower. You also want to ensure you have lockout thresholds for failed logins to any accounts. If an attacker is attempting various password attacks, this may at least slow them down whilst you react to alerts.

In terms of detection's, there are a number of things we want to look for. Do your best to ensure all perimeter facing devices are on boarded to your SIEM so you can monitor authentication events.

> **Password Spraying –** Create an alert looking for one Source IP failing to login to 5+ Accounts within 20 minutes. (This is just an example, you will need to modify the thresholds depending on the log type and your environment.)
>
> **Impossible Travel –** Most SIEM's have a function to detect the geographic location of IP addresses. Monitor if a user account logs in successfully from 2 different countries within an hour. (You may need to allowlist any VPN providers which are commonly used by your user base)

Attempted user login from multiple Sources – A sign of potentially leaked user credentials or password cracking is when there is numerous successful or failed logins to one user account from multiple IPs in a day. Create an alert looking for 5 IPs successfully or failing to login to the same user account in a 24 hour period (As previous, you may need to alert thresholds depending on your environment and risk appetite)

Other – It is also worth looking at creating rules looking for large numbers of failed logins to one account, large numbers of failed logins from one source and large numbers of failed logins to one destination. The thresholds and exceptions you will use for these will depend greatly on what you are monitoring and your environment. Run some queries, find what is normal and alert above that.

Finally for this section, it is mentioned in the report that attackers may have used a vulnerability in SonicWall to disable MFA on the VPN.

I always recommend that you audit change events on any networking equipment in your environment. You likely have VPN's, Firewall's and a plethora of other networking equipment logging network traffic and authentications – keep sure you are also auditing and logging change activities on these too.

Look for events such as deletions, creations and modifications of objects, policies and accounts on these devices. Alert on them and ensure that any changes are legitimate and expected.

Malicious Emails

It is mentioned that another initial access vector was, unsurprisingly; malicious emails.

I'm not going to cover email security and all its facets here. Rather, this tweet from @TinkerSec at the time sums up up the basics pretty well. Look into each of these aspects separately and see if you have them, or a direct alternative; in place.

> So plan on it.
>
> – Use email security proxies to conduct scans of attachments ahead of time.
> – Use endpoint protection.
> – Use outbound domain inspection.
>
> – Have a way for users to report phishes.
> – Don't punish users if they self report.
>
> — Tinker (@TinkerSec) May 11, 2021

ESTABLISH FOOTHOLD

BEACON

This is mentioned in this phase and also for lateral movement, but I will just include it here. Beacon / Cobaltstrike is now known for being used in a large number of intrusions to perform numerous functions (which you can learn about in the below link)

To hunt for it, detect it or are looking for IOCs, this is your go-to link.

Awesome-CobaltStrike-Defense contains the following topics and is regularly updated.

- Hunting and Detection Tools
- Yara Rules
- Sigma Rules
- IOCs
- Research articles
- Trainings
- Videos

MAINTAIN PERSISTENCE

Teamviewer / Anydesk and other remote acccess applications

The report shows us that the threat actor downloaded and used Teamviewer. They also browsed to locations indicating downloads of Anydesk. I would recommend that, if possible; your business mandates one remote access application which is allowed to be used. Then, anything outside this is immediately suspicious.

In terms of alerting, we should approach this from two avenues. Firstly, I recommend you look for outbound connections on the following ports which are used by common remote access applications.

RDP – 3389
Anydesk – 6568
Dameware – 6129, 6130, 6132, 6133
Teamviewer – 5938
VNC – 5800/5900

If your business does mandate the use of one, or no; remote access applications. Block the download links for these and then alert if there is a blocked connection to these download URLs (such as hxxps://dl.teamviewer[.]com/download)

Legitimate Credentials

This is difficult to deal with and is a huge challenge that we face, as threat actors purchase working user credentials and log directly into systems. There is some steps that we can take however.

- Firstly, sign up for domain monitoring on haveibeenpwned. If an employees credentials are breached, ensure that they reset their password to a new, complete different one.
- Inform users to create unique, lengthy passwords for all services. Therefore, if an attackers does buy a credential it will only work on one of the applications / services etc.
- I mentioned it already, but MFA on everything. Then, if a password is breached, you have another layer of defense.

In terms of detection's, for this we really need to look at anomalous behaviour patterns, such as.

- Users accessing, or attempting to access; a host they have never accessed before.
- User logging or attempting to login outside of their normal working hours.
- Mentioned already above, but Impossible Travel scenarios can be a good way of catching legtimate credentials being used.
- For your critical servers / hosts (Domain Controllers, Network Devices, Exchange Servers, Databases etc – *whatever you consider critical)* you should know who (Domain Admins, Network Admins etc) is allowed to access these. Create an alert if any users outside this accesses, or attempts to access; your critical servers and hosts.

ESCALATE PRIVILEGES

Mimikatz

Mimikatz is another tool which commonly used during many attacks, especially for privilege escalation.

Due to its common usage, it is worth taking your time to mitigate as many potential attacks as possible. The following articles detail numerous mitigation's which can be taken against Mimikatz.

SANS – Mitigations against Mimikatz style attacks.

Tempest Security – Mitigating credential theft attacks.

Once you have mitigated potential issues, it is then worth implementing the below detection's. Mimikatz does so much it is hard to list a detection for everything that it can do, so here are the more common ones.

There are 3 good Sysmon detection's in this Medium post.

Sigma rule to detect well-known mimikatz command line arguments

Sigma rule to detect mimikatz keywords in different Windows Eventlogs

Mimikatz DC Sync. (When Mimikatz is used to perform DCSync) EventID 4662, Properties contain *Replicating Directory Changes All* and/or *1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*

Mimikatz Detection LSASS Access (Mimikatz normal behaviour) Sysmon Event 10, Target Image C:\windows\system32\lsass.exe, Granted Access"0x1410"

Credential Dumping Service Execution. (Looking for services known to be used to dump credentials) Event ID 7045 or 4697 and ServiceName contains "Mimikatz or mimidrv or gsecdump or cachedump or pwdump or wce service or wceservice or fgexec."

OverPass The Hash. (Detection of successful overpass the hash attack) Event ID = 4624, Logon Type = 9, Logon Process Name = seclogo, Authentication Package = Negotiate

LSASS Memory Dump

Commonly at this phase of an attack, attackers will look to dump the memory from LSASS and other attacks against the service.

I highly recommend reading this threat detection report by RedCanary. It explains well what LSASS is, why it is attacked so frequently and several detection's for these attacks.

I also recommend reviewing the MITRE sub technique – OS Credential Dumping: LSASS Memory . This provides further extra information and resources around what LSASS is, potential mitigation's and detection's.

Some detection's which are relating to LSASS below (I also listed some in the previous section as Mimikatz targets LSASS)

LSASS Access from Non System Account. EventID 4663 or 4665. Object Type = Process, Object Name ends with lsass.exe. SubjectUsername does not end with $.

Password Dumper activity on LSASS. EventID 4656. Process Name = C:\Windows\System32\lsass.exe. AccessMask = 0x705. ObjectType = SAM_DOMAIN.

LSASS Memory Dumping. Windows Process Creation. CommandLine contains lsass and .dmp. CommandLine does not end with .werfault.exe OR CommandLine does not end with .exe and contain procdump.

MOVE LATERALLY

RDP

RDP has been used extensively by many threat actors for lateral movement among other purposes, therefore it is important we monitor its the best we can.

But before we get to the detection stage, as always lets first try to mitigate. MITRE have some fantastic mitgations listed here which I highly recommend following to deter and make an attackers life more difficult.

Now onto the detection's. RDP is such a frequently used protocol during attacks, so I am going to list a bunch of my favourites below which I recommend looking into.

> **User RDP Spike.** Alert on a user making numerous RDP connections in a short period.
>
> **Abnormal RDP Access.** Alert on devices being accessed via RDP which are not normally accessed using the protocol.
>
> **Source with many Destinations.** Alert on a Source IP with a large number of Destination IPs in a 24 hour period using RDP.
>
> **Possible RDP Tunneling.** Look for EventID 4624, Logon Type 10, Source Address = 127.0.0.1 or ::1
>
> **Netsh RDP Port Forwarding.** Look for EventID 4688 where CommandLine = netsh i* p*=3389 c*
>
> **Potential tsclient being used to place RDP Backdoor.** Sysmon Event 11, Image: '\mstsc.exe', TargetFileName: '\Microsoft\Windows\Start Menu\Programs\Startup*'
>
> **Suspicious Outbound RDP Connections.** Sysmon Event 3, Destination Port 3389. Image is not any of mstsc.exe, RTSApp.exe, RTS2App.exe, RDCMan.exe, ws_TunnelService.exe, RSSensor.exe, RemoteDesktopManagerFree.exe, RemoteDesktopManager.exe, RemoteDesktopManager64.exe, mRemoteNG.exe, mRemote.exe, Terminals.exe, spiceworks-finder.exe, FSDiscovery.exe, FSAssessment.exe, MobaRTE.exe, chrome.exe, thor.exe, thor64.exe.

INTERNAL RECONNAISSANCE

Powerview / Bloodhound

Threat actors commonly use tools such as Powerview and Bloodhound to perform internal recon against Windows targets.

My main recommendation here? Run them yourself first. Find and fix the weaknesses before they do. I discussed Active Directory Security Hardening, Auditing and Detection Rules on a post a while ago. I recommend giving it a read and following the steps outlined within.

There are some SIEM rules which we can look to implement to pick up the activity from these tools.

> **Powerview Add-DomainObjectAcl DCSync AD Extend Right. (**Detects PowerView being used to grant DCSync permissions to a user. Only false positve is if a new DC Account is being created**)** EventID 5136. LDAPDisplayName = ntSecurityDescriptor. Value contains either 1131f6ad-9c07-11d1-f79f-00c04fc2dcd2 OR 1131f6aa-9c07-11d1-f79f-00c04fc2dcd2 OR 89e95b76-444d-4c62-991a-0facbeda640c.
>
> **Use of Bloodhound and Sharphound.** There is a nice Sigma rule here.

Built in Windows Utilities

Frequently we see threat actors using built in Windows utilities to aid their reconnaissance and attacks in general. Outside of this incident, we can also see this when we look at reports from the likes of TheDFIRReport. Almost every post, there is evidence of an attacker using these in built utilities.

Therefore, we have to try and detect this. Between the DFIRReport link above and JPCert – Windows Commands used by Attackers we can quickly build a list of frequently used commands.

It is worth taking these commands and creating a rule looking for a user running 5+ of them in 5 minutes. (You may need to change your thresholds). You will need to allow list Domain Admins, Network Admins and potentially other staff members depending on role.

On top of this, there are a number of other good built in recon rules which can be found in this Sigma repository and search for recon.

Advanced IP Scanner

During most reconnaissance attackers will run various network scans to fingerprint the target environment and find vulnerable devices, open ports etc.

Before we get into the detection's, the best mitigation here is to ensure only required ports are open on devices. This will limit what an attacker can find out about your devices, or at least make the job more difficult in the worst case.

It is therefore important that we monitor for suspicious network activity. I wrote this blog post a while back, it needs updated but contains some basic logic around network monitoring. If you have DNS logs, also take a look at this post.

On top of the two above articles you should also be looking for things such as –

- Telnet / SSH – Source IP with many destinations in a day (Strange – these is a management port – investigate why)
- Abnormal spike in traffic from a host. Either based on Event Count and/or Data Volume. This can be abnormal either to your environment, subnet or the host itself compared to its previous traffic.
- Basic Port Scans within your network. Look at internal traffic only. Then alert on if 1 Source IP connects to either 100 destinations on the same port within 5 minutes or 1 destination over 100 ports in 5 minutes. (These thresholds may need modified and you may need to allowlist certain devices such as vulnerability scanners)

COMPLETE MISSION

PSExec

PSExec has been seen during DarkSide ransomware attacks to deploy the ransomware itself.

In terms of what PSExec is, why threat actors use it and how we can detect it; the following two posts are fantastic.

Firstly, Praetorian – Threat Hunting: How to Detect PsExec. This contains details on what it is, how to detect, variants of PSExec and further considerations.

Next up, another great RedCanary post. Threat Hunting for PsExec, Open-Source Clones, and Other Lateral Movement Tools. This contains similar detail on PSExec but goes on to focus on the many clones of PSExed, what they are, and how we can detect them also.

FINAL THOUGHTS

Before we finish, I have some final thoughts which I thought were best to mention at the end rather than throughout the rest of the post.

Patch – I know this can be easier said than done at times, but it can be the difference between being breached, and not. Most attacks, if the breach itself wasn't due to a vulnerability; the attackers was able as part of their attack chain to exploit some vulnerability to speed up their attack or bypass defenses. Do your best to limit their opportunities to do this.

Test your prevention's and detection's – Once you have mitigation's and detection's in place, test them. Are things really being blocked? Do alerts really trigger in your SIEM? Testing your hard work is a vital step in the process which should never be skipped.

Response – If a serious incident does occur – do you have an IR team? Do you have one on retainer? Have you played out scenarios and went through the how, who and why you will respond to a real event? There are some fantastic Incident Response resources here.

Thanks for taking your time to read this blog post and I hope you found it useful. I always love feedback, so contact me at My Twitter if you want to discuss this article, or anything related.

Leave a Reply

Your email address will not be published. Required fields are marked *