Blue Team Detection: DarkSide Ransomware

By Secprentice

Published: 2021-06-13 · Archived: 2026-04-06 01:17:40 UTC

Featured

Malware write-ups can be found in abundance online, they are often written from the point of view of a malware researcher who focuses on the deep internals of how malicious software works.

- Secprentice

  Blue Team Detection: DarkSide Ransomware

Malware write-ups can be found in abundance online, they are often written from the point of view of a malware researcher who focuses on the deep internals of how malicious software works, in some cases the information provided cannot be used to derive actionable intelligence and defence mechanisms by cybersecurity blue teams. With that said, Researchers normally publish lists of hashes, file names, paths and IP addresses but these are easily rotated by attackers and therefore quickly become redundant for defenders. So, instead of looking for these fingerprints (which frequently change), we should instead look to detect malware by its *behaviours (which are relatively persistent and common across many malware flavours)*. In this post, I hope to take a recent popular strain of malware and pick it apart, not as a malware analyst but as a blue team defender to create intelligence that can be used to detect malware based on its generalised behaviours instead of a stagnant list of hashes, IPs or file names.

DarkSide Ransomware unleashed chaos on the Oil industry recently by demanding millions of dollars to decrypt critical infrastructure networks. Thankfully Fireye has written up a great report which illuminates some of the tactics employed by Darkside admins to inflict their cryptographic nightmare. Although it seems Darkside is making a swift exit the methods they use are common across many threat actors and therefore the advice below remains applicable to other ransomware flavours.

> Based on the evidence that DARKSIDE ransomware is distributed by multiple actors, we anticipate that the TTPs used throughout incidents associated with this ransomware will continue to vary somewhat

https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

Detection Opportunities

Image credit: Fireeye

#1 Password attacks at the perimeter

Consumers of security tools are often led to believe that Ransomware is a complex threat but for our first detection opportunity, we see quite the opposite.

> In multiple cases we have observed suspicious authentication attempts against corporate VPN infrastructure immediately prior to the start of interactive intrusion operations. The authentication patterns were consistent with a password spraying attack, though available forensic evidence was insufficient to definitively attribute this precursor activity to UNC2628. In cases where evidence was available, the threat actor appeared to obtain initial access through corporate VPN infrastructure using legitimate credentials.

The attackers are simply logging into the victims VPN appliance and accessing the network where they assume the permissions of the user whose credentials they have stolen. This isn't a complex intrusion. It's just logging in. It could have been slowed or perhaps stopped by modernising password policy and enabling two-factor authentication on the VPN gateway.

Defenders can detect this stage of the attack by monitoring VPN authentication logs (normally Syslog directly from the VPN appliances or RADIUS) for multiple failed attempts. Also, multiple failed attempts followed by success. Alert fidelity can be achieved in modern SIEMs by applying baselining or machine learning to automatically detect anomalous authentication instead of relying on a static threshold such as X auth failures in Y minutes.

Simplification of the attack for visual learners.

FireEye does also mention the attacker may have logged in with legitimate credentials, it could be argued that the attackers stole or were sold a working username/password combination. In this case, it's surely safe to assume that two-factor authentication would have slowed down the attackers. Implementing 2FA is initially time-consuming but a breeze to work with after the initial deployment hump. Some say that user workflow and productivity is hampered by having a two-factor authentication process but thanks to modern push notification solutions (like Duo and Azure) this simply isn't true. Your smartphone can send you a push notification that you tap and unlock with biometrics adding fractions of a second onto your login time. The pros of a more secure VPN outweigh the cons of a few extra seconds of logon time.

#2 Exploitation of edge appliances.

Admittedly this section is only half a detection, the other half is patching advice.

FireEye noted that some Darkside attacks exploited CVE-2021-20016 for initial access. This vulnerability allows unauthenticated remote commands to be executed against SonicWall appliances. Anyone with an internet connection and the right set of instructions (SQL queries in this case) can easily steal credentials from the SonicWall appliance and use them to break into a network from the outside. This low effort, high yield attack is made possible by the precarious location of edge networking appliances, bridging the internal and external network.

Simplification of VPN appliances on the internet.

If your network has any edge appliances (Citrix, VPNs or similar) they must be promptly patched when vulnerabilities are disclosed, the sooner the better. Failing to do so will undoubtedly allow attackers in eventually. It's possible to detect such vulnerabilities with an external vulnerability scanner or simply by signing up for a notification service like https://secalerts.co.

In some cases, it's also possible to detect appliance attacks via their logs although this varies by vendor and vulnerability. Knowing which logs to look at isn't always known until long after the vulnerability has been published. In most cases, the appliance will write a Syslog message or have a particular file in a particular location that shows the system has been compromised. It's probably best not to count on this method for detecting networking appliance intrusions. Prevention is better than the cure.

#3 Phishing

A group that Fireye have dubbed UNC2465 snuck Darkside in via the "Hamhock" backdoor. It's hard to find much information about this backdoor other than what's provided in the Fireye write up but it's possible to make educated guesses about its tactics based on the snippets of information Fireye have included.

> During one incident, the threat actor appeared to establish a line of communication with the victim before sending a malicious Google Drive link delivering an archive containing an LNK downloader. More recent UNC2465 emails have used Dropbox links with a ZIP archive containing malicious LNK files that, when executed, would ultimately lead to SMOKEDHAM being downloaded onto the system

So, UNC2465 delivered the Hamhock backdoor via phishing in two flavours. One using cloud storage services like Google Drive or Dropbox and the other by hiding malicious LNK files inside ZIPs and sending them directly to the victim. Fireeye has not shared many details about the phishing kill chain but we can safely assume it looks something like these Any.Run samples that abuse LNK files:
https://app.any.run/tasks/2f776569-a3be-42e4-a6af-732982c9b2ed/
https://app.any.run/tasks/2f776569-a3be-42e4-a6af-732982c9b2ed/

When boiled down this phishing attack is nothing more than delivering a shortcut file that points towards a malicious command. The shortcut file is put in front of the user inside of a ZIP file attachment or hidden behind a cloud file sharing link.
This isn't anything new and certainly isn't anything to be concerned about because long kill chains like this grant many detection and prevention opportunities for us defenders.

A rough outline of the LNK kill chain as per AnyRun samples.

To detect and prevent this phishing method defenders should consider some or all of the following actions:

- Do not allow LNK files to be delivered as eMail attachments. Block LNK files from being delivered to end-users.
- Ensure that this block extends to LNK files inside of ZIPs. Most modern email gateways can look inside ZIP files for malicious files.

- Ensure that this block extends to LNK files inside of encrypted ZIPs. Attackers sometimes password-protect ZIP files to stop eMail scanners from looking inside. This particular protection may interrupt normal business workflows and therefore is not suitable for everyone, your business should be consulted for appetite first.
- Use EDR to monitor for archive software (WinZip, 7Zip, Unrar) writing .LNK files to disk aka being extracted.
- User EDR to monitor for a suspicious parent to child process relationships as per any other malware. For example: CMD.exe > MSHTA.exe > PowerShell.exe. There's no special sauce here. Once the attackers are on the network they still rely on traditional code execution and foothold techniques, so stick to what you know and don't be distracted by the fact that a new scary ransomware flavour is involved.

#4 Privilege escalation detection

After any hacker has gotten into her target network she will want to obtain high privileges so she can spread deep into the network and encrypt as many systems as possible. Again, there is no secret sauce here. The ransomware operators are using the same tried and true techniques. Specifically called out by FireEye are Mimikatz, CVE-2020-1472 and LSASS memory dumps. To detect and prevent these privilege escalation attacks, defenders should implement as many of the below initiatives as possible:

- Patch systems regularly and promptly. CVE-2020-1472 can be avoided by installing patches.
- Administrators must ensure that wdigest regkey is set to 0 on systems running Windows 7, 8, Server 2008, and Server 2012. This stops plain text credentials from being stored in memory. EDR tools should be used to monitor for modifications to the wdigest registry key as attackers may try to modify it to weaken system security
- Administrators should also ensure the **RunAsPPL** registry key is set which stops tools like Mimikatz from dumping the LSASS process memory where credentials are stored in a hashed format.
- As mentioned earlier, password policies must be modernised with length and longevity in mind.
- A large portion of common Microsoft domain attacks can be detected by Microsoft ATA, now renamed to Microsoft Defender For Identity.
  The agent runs on domain controllers where it can monitor for suspicious behaviour in domain controller logs.

#5 Monitoring and controlling administrative tools

All of the hacking groups that deployed DarkSide were observed by Fireeye to be using system administrator tools that have no place on a network except in very particular circumstances. Defenders should look to strictly control access to the following tools:

- Teamviewer
- rClone
- PSExec

FireEye directly calls out the fact that the attackers downloaded standard binaries for these tools directly from the vendor source. (For example dl.teamviewer.com) This is interesting because it highlights the fact that the attackers

don't feel the need to hide this download, obviously because it often goes undetected.
Defenders can detect and control the use of these tools using EDR Watchlists, Firewalls and application control tools like AppLocker. If a user starts any of these applications without proper permission or explanation their activity should be investigated.

#5 Protect ESXi

> Mandiant observed the threat actor navigate to ESXi administration interfaces and disable snapshot features prior to the ransomware encryptor deployment, which affected several VM images.

I believe this claim to be profound because this isn't a commonly talked about attack vector and few organisations are properly monitoring their virtual machine management consoles. Defenders should work to implement as many of the following recommendations as possible to protect their ESXi hosts from attacks like this.

- Ensure that all virtual machine hosts are patched and running the latest software available from the vendor. If you don't have a vulnerability management platform then sign up to a service like https://secalerts.co/ for email alerts.
- Control access to your ESXi hosts tightly, only share the credentials with employees who need to know. Be sure to rotate the passwords after key administrators leave the company.
- Set long complex passwords for your ESXi server backends and store them in password vaults like Secret Server, KeePass or BitWarden.
- Monitor ESXI Syslog for multiple authentication failure events in a short period of time.
- Ingest your ESXi Syslog logs into a monitoring platform and configure alarms that will warn you of virtual machine snapshots being deleted in bulk.

This week's images were provided by Nina Z's digital art collection.

Help Support Our Non-Profit Mission

If you enjoyed this article or found it helpful, please consider **donating**. Secjuice is a 501(c)(6) non-profit and volunteer-based publication powered by donations. We will use your donation to cover our hosting costs and **keep Secjuice an advertisement and sponsor-free zone**.

Donate at Open Collective
