DARKSIDE, INC. EXPLOITS

Security Audit

Mark Ennis
October 6th, 2022

Executive Summary

The cybercriminal group, Darkside, Inc. has been launching ransomware attacks against companies. These attacks result in data exfiltration, and compromised systems have their files encrypted. The attacks are careful to avoid detection in order to maximize their eventual impact. The attackers avoid endpoints that are monitored more closely for that reason. Each attack is highly targeted and involves custom code as well as varied techniques for gaining access. Once they have access to a machine, they install backdoors and gather as much information as possible. User data, credentials, and confidential files are all downloaded from compromised systems. Once the data has been exfiltrated, they have elevated their privileges and gained as much information about resources on the network, the attackers encrypt the machines. The data and encrypted files are held for ransom until the organization pays the attackers. Defending against these attacks is extremely difficult due to their unique and varied nature. Creating an organization with stringent cybersecurity policies and robust security culture is the best defence.

Introduction

Since 2020, ransomware attacks by the group known as Darkside, Inc. are on the rise. They perform highly targeted and customized attacks on organizations. They appear to be a skilled organization that avoids attacking hardened endpoints and hides their tracks well. The attacks have two effects. Firstly, they exfiltrate sensitive data from the systems they compromise. Then, the files on the system are encrypted. In order for an organization to regain access to its files and prevent its data from being leaked, it must pay Darkside.

For the purposes of simplicity, Darkside, Inc. will be referred to as Darkside or “the attackers” throughout this document.

Body

Discovery

Darkside attacks are discovered when the victim finds that the files on their machines are encrypted. A text file is created on the compromised instructions with instructions on how to contact the ransomware creators. Then, the victim can pay Darkside to be able to decrypt the files.

Darkside attacks take pains to avoid early detection. They avoid machines running Endpoint Detection and Response (EDR) software. They use custom code and extensions in order to avoid signature-based detection. Signature-based detection techniques can easily identify patterns of actions, checksums, or other common elements in widely used malicious software. By customizing the code for different attacks they are able to avoid this form of detection.

Vulnerabilities

Darkside is able to access systems and accounts that are remotely accessible. Throughout the pandemic, with the rise of remote work, they have targeted Virtual Desktop Infrastructure (VDI). VDI allows remote users to access virtual machines through a graphical interface. They also target public-facing servers. Their attacks are heavily targeted and require different approaches depending on the target. It is likely that they performed some brute force password cracking attacks, employed credential-based attacks based on stolen data, exploited application-level vulnerabilities, and used social engineering to gain access to different systems.

It is worth noting that the attackers noticed some network security measures and have taken pains to avoid them. Machines that were protected by EDR were not targeted. EDR tools refer to a combination of host-based security tools such as HIPS/HIDS, anti-virus, file encryption, anti-ransomware tooling, and more. Additional protection can be granted from these attacks by securing machines. The attacker will avoid the machine and choose softer targets in order to avoid detection and complete their attack.

Exploits

Once they are inside a network, they explore and exfiltrate sensitive data. Darkside commonly employs Living-off-the-Land (LotL) techniques. Rather than executing their own malicious code LotL attacks rely on tools and services that are already present in the victim's environment. LotL attacks are harder to detect because the tools they use are a known quantity and their execution is less suspicious. Using these techniques they are able to access user information, sensitive data, credentials, and environment information. Some of this information is vital for the later stages of the attack.

Additionally, backdoors are installed on compromised systems to enable Command-and-Control (C2). A Remote Desktop Protocol (RDP) connection is set up through a Tor browser that runs as a persistent service on the compromised machine. RDP is a protocol that allows users to use a graphical desktop on remote Windows machines. The RDP connection is established on port 443, from a dynamically generated port on the local machine, so that it is indistinguishable from normal HTTPS traffic. The connection is routed through TOR to help the attackers remain anonymous.

A secondary C2 mechanism is set up using Cobalt Strike. Cobalt Strike is a remote penetration testing tool that allows the attacker to perform Operating System Command Execution (OSCE), key-logging, file transfers, port scanning, and many other functions. They do this by deploying custom stagers to machines using Windows Remote Management (WinRM). WinRM allows for the deployment of applications across a network. The stagers deploy a beacon. In Cobalt Strike, beacons connect to a C2 server and give the attacker access to the full suite of penetration testing functionality.

Once they have created a backdoor, they begin exfiltrating data. They search for confidential files, credentials, keyboard history, and user data. They archive and compress the data before sending it out. After they have downloaded the victim's data, they can begin the ransomware attack.

The ransomware attack is two-pronged. First, all of the victim's files have been encrypted and are no longer accessible. Any data that has not been backed up to a secure location that has not been compromised by the attackers will be completely inaccessible. However, a victim may have copies of these files, or they may decide that the value of the data is less than what they must pay to the attackers. In order to further incentivize payment, the attackers also export credentials and files. Failing to pay the attackers will also result in the exfiltrated data being posted publicly.

Attack Vectors

These attackers target public-facing machines. This includes VDI and other ways for employees and contractors to connect to a company network. It also includes servers running applications that need to be accessed from the outside. Once they have compromised a node within a network, they will work on accessing other accounts, machines, and adjacent networks. All of these attacks do begin from a remote location. Defending against these attacks means keeping servers and applications patched to minimize vulnerabilities, requiring MFA for remote access to strengthen Access Control, and making as few of these systems externally visible as possible to reduce the possible attack service.

Once the attackers have gained access to a network, mapped out the important servers and applications, and compromised privileged accounts, they deploy their ransomware. The ransomware is deployed via one of the backdoors installed by the attackers, either Cobalt Strike or RDP-over-TOR. At this point, data will have been exfiltrated already, and the attacker will attempt to encrypt the system as fast as possible. Up until this point, the attackers have been attempting to avoid detection as much as possible. Once the ransomware begins to encrypt the system, without an EDR with anti-ransomware functionality the victim is defenseless.

Severity

The ransomware attacks and the data exfiltration in Darkside attacks are of critical severity. The attackers gain administrator access and get password data for the entire domain. The integrity of all machines in a network compromised by these attacks is suspect. Additionally, there has been a complete loss of confidentiality in the system. The attackers have managed to exfiltrate sensitive files, credentials, and data. Lastly, the attacker is able to deny access to all of the resources on the compromised machines by encrypting them. This results in a loss of availability for the compromised system.

Using the FIRST CVSS calculator, the attack has a score of 8.5 / 10. It would score higher, but the attack is highly complex and requires a high level of technical skill.

Impact

The impact of the Darkside attacks is high. In order to regain access to the encrypted systems, a victim is forced to pay a presumably substantial sum to the attackers. Alternatively, they can choose not to pay, lose the files in encrypted systems, and have their confidential data leaked. Either way, the company will be forced to treat its systems as compromised. They will likely need to be rebuilt in a clean environment to ensure no more back doors remain. Additionally, they will need to perform a security audit of all their assets to ensure that whatever vulnerabilities were exploited have been closed. Regardless of whether or not they pay the attackers, the confidentiality of their systems has been completely compromised. An organization cannot consider any data that was on the systems secure going forward. The disruption to business will be high, as will the economic costs.

Reconnaissance

Passive Reconnaissance

Given some of their public statements, it appears that Darkside performs a high level of reconnaissance before an attack. They are selecting their targets carefully. They are avoiding public-sector and health-care organizations. They are performing financial analyses on companies before launching their attacks. This indicates they are researching publicly available information to build a profile of potential victims. They are likely pulling lists of records from domain-name registrars and attempting to find out what services and infrastructure the company uses. Although some of that can be found with active reconnaissance, much of that information is also posted in marketing materials, developer blogs, and other companies web sites. Additionally, they are likely to engage in forms of social engineering. They could be researching and reaching out to employees to learn more about the company.

Active Reconnaissance

Depending on how the attackers gained access to a system, any number of Active Reconnaissance techniques could be employed. They are likely engaging in port scanning, web scanning, and fingerprinting techniques in order to identify vulnerable machines they can use to enter the network. Brute force attacks are employed to break into services not protected by MFA or an IPS. It is likely that Darkside attackers have gained entry through services with default configurations and credentials. They have probably found Application Level exploits that allow them to gain access to a system. They have performed phishing attempts and other targeted attacks against users. They are also checking systems for EDR and other cybersecurity measures. Given the highly targeted nature of the attacks, the attackers are likely employing all methods of reconnaissance available to them.

Conclusions

Defending against Darkside attacks will be difficult. Given the targeted and custom-built attacks performed on each organization, there is no single preventative solution. Encouraging a security culture within a company is the best defense. Policies should be put in place to regularly patch and update systems. Employees should be educated in security awareness in order to help reduce their vulnerability. Users should be given access according to the principles of Least Privilege so that when accounts are compromised the scope of the damage is limited. Valuable and important nodes should be hardened by employing EDR tools. By making a system more difficult to compromise, attackers will look to softer, easier targets.