Threat Discovery

Stages of a Ransomware Attack

DARKTRACE

Ransomware is a multi-stage problem. Darktrace is the only vendor with the multi-stage solution that autonomously and effectively contains the attack at any stage and ensures the attacker cannot progress.

1. INITIATION

1. Initiation | 2. Establish Foothold & Beaconing (C2) | 3. Lateral Movement | 4. Data Exfiltration | 5. Data Encryption | 6. Ransom - $ | 7. Clean up & Recovery - $$$ | 8. The Cycle Repeats

To accomplish the initial entry, the attacker may launch their attack via a spear phishing email, RDP brute forcing (exposed internet service), malicious websites and drive-by downloads, an insider threat with company credentials, system and software vulnerabilities, or any number of other attack vectors. By constantly looking for novel ways into digital environments, attackers stay ahead of threat intelligence and can avoid traditional defenses. Just a single small vulnerability or oversight is enough for a threat actor to perform an initial compromise. Once the initial breach has been achieved and they find themselves inside an organization's network, a massive range of attack vectors are opened up to attackers.

Legacy Security Solutions

If the initial breach is a simple, historical attack, it might be stopped. If it is one of the vast, ever-increasing number of sophisticated and novel attacks being launched, it can continue onto the next stage.

Attackers will often purchase the off-the-shelf defenses to test their malware against to see if it will be effective. If the malware is brand new, it will likely pass these checks against all legacy solutions.

Secure Email Gateway

Malicious links and attachments

Phishing (e.g. for credentials)

Catch only when seen before

Firewall

- Requires configuration on a per-organization basis, often modified based on the needs of the business.
- If the attack hits firewall where a rule or signature does not match it, it will bypass the firewall.

Endpoint Antivirus

- In cases of malware downloads, endpoint antivirus will detect these if, and only if, the malware has been seen and fingerprinted before.

IDS/IPS

- Looks for known malware being downloaded, leverages pre-programmed rules and uses pre-programmed responses.
- Rarely get deployed as they often do more harm than good, causing more disruption.
- Looks at pre-defined patterns. Relies on a new attack to have sufficiently similar traits to attacks that have been seen before.

Darktrace's Autonomous Response

Breaches inherently break from a digital estate's normal 'pattern of life' and can therefore be detected by Darktrace. Once detected, they are stopped at this early stage by Autonomous Response. This includes sophisticated attacks like spear phishing. Action taken is tailored and precise, meaning no disruption is suffered by the business. With Darktrace, ransomware attacks end here, but its Autonomous Response capabilities work at later stages as well.

Secure Email Gateway	Proportionate, progressive actions
Email › Out of Character › Suspicious link › Suspicious Attachment › Solicitation › Extortion › Spoofing **Network** › Unusual Incoming RDP › Unusual file download › Unusual .exe fileTorrenting	Darktrace constantly reassesses your business and adjusts its response based on new evidence and actions by an attacker. ✓ Lock or Double Link ✓ Convert or Strip Attachment ✓ Hold Message ✓ Unspoof ✓ Block specific connections E.g. Port 3389 to IP xyz.xyz.xyz Darktrace can determine which connections to block, even if the port, protocol, or IPs have never before been seen or used maliciously ✓ Enforce pattern of life ✓ Enforce group pattern of life

BRINGING THE HUMAN INTO THE LOOP

AI Analyst Investigations — At every stage, the Cyber AI Analyst replicates the human analyst's ability to piece together attack narratives, surfacing and triaging significant incidents.

Proactive Threat Notifications (PTN) — Darktrace's SOC, made up of over 100 cyber analysts, investigates the most pressing incidents and raises high-priority alerts directly with the people who need to know.

THIS ATTACK WOULD NOT HAVE PROGRESSED

2. ESTABLISH FOOTHOLD & BEACONING (C2)

1. Initiation | **2. Establish Foothold & Beaconing (C2)** | 3. Lateral Movement | 4. Data Exfiltration | 5. Data Encryption | 6. Ransom - $ | 7. Clean up & Recovery - $$$ | 8. The Cycle Repeats

At this stage, the attacker makes contact with the breached device(s), allowing them to control subsequent stages of the attack remotely. During these Command and Control (C2) communications, further malware may also pass from the attacker to the devices. This helps them to establish a foothold within the organization and readies them for lateral movement.

Legacy Security Solutions

Traditional defenses tend to be blind to Living off the Land tactics, whereby an attacker leverages existing, standard business practices to compromise an environment.

Firewall & IDS/IPS

These systems tend to look at connections in isolation, rather than in the context of previous and potentially relevant connections, thereby making differentiation from normal traffic difficult. They may block 'known-bad' domains or use some geo-blocking, but this is where an attacker would likely live off the land as well as leverage new infrastructure.

These tools also don't tend to analyze for things like the periodicity, like whether a connection is beaconing at a regular or irregular interval, or the age and rarity of the domain in the context of the environment.

Darktrace's Autonomous Response

Suspicious C2 connections and the downloads which follow them are spotted, even when conducted using regular programs or methods.

Once they are detected as a threat, Autonomous Response halts these connections and downloads but allows normal business activity to continue.

Potential unusual activity	Potential actions
› Anomalous connections › Connections to unusual endpoint › Anomalous file downloads › Beaconing activity to external rare endpoint › Beacon to young endpoint › SSL or HTTP beaconing to rare destination › Incoming remote desktop › Unusual data download from rare destination › Unusual data upload to rare destinatio	✓ Block specific connections ✓ Enforce pattern of life E.g. as a device makes new connections, allow the legitimate, usual connections to continue while quickly neutralizing any unusual events. This is only possible when you understand 'self' ✓ Enforce group pattern of life E.g. Prevent this device from doing anything its peers haven't done

BRINGING THE HUMAN INTO THE LOOP

AI Analyst Investigations | Proactive Threat Notifications (PTN)

THIS ATTACK WOULD NOT HAVE PROGRESSED

3. LATERAL MOVEMENT

1. Initiation | 2. Establish Foothold & Beaconing (C2) | **3. Lateral Movement** | 4. Data Exfiltration | 5. Data Encryption | 6. Ransom - $ | 7. Clean up & Recovery - $$$ | 8. The Cycle Repeats

Once an attacker has established a foothold within an organization, they begin to increase their knowledge of the wider digital estate and their presence within it. This is how they will find and access the files which they will ultimately attempt to exfiltrate and encrypt. It begins with scanning the network, building up a picture of its component devices, and then moving laterally. The attacker infects more devices and often looks to escalate their privileges – for instance by obtaining admin credentials – thereby increasing their control over the environment. Once they have obtained authority and presence within the digital estate, they can progress to the final stages of the attack.

Legacy Security Solutions

Because they rely upon static rules and signatures, legacy solutions struggle to prevent lateral movement and privilege escalation without also impeding essential business operations. Novel methods of movement, including Living off the Land techniques, will be difficult for these approaches to stop.

Firewall & Network Access Control (NAC)

In theory, an organization leveraging firewalls and NAC internally with proper network segmentation and a perfect configuration could prevent cross-network lateral movement.

In reality, validating the efficacy of such a configuration is extremely difficult, however, and maintaining a perfect balance between protective and disruptive controls near impossible.

IDS/IPS

- IPS denies network traffic when known threats are detected in packets, therefore requires the database to be constantly updated with new threats.
- Both IDS and IPS sit at the ingress/egress points so cannot see lateral movement.
- An IDS may sit out-of-line but without response capabilities.
- An IPS may sit inline which means when two devices communicate via alternative pathways, they are out of scope of both detection & response.
- A full NIPS (Network Intrusion Protection System) might ingest all internal traffic and has the ability to block internal connections but suffers from the same limitations of IPS.

Darktrace's Autonomous Response

Even familiar programs will be flagged by Darktrace if used maliciously by attackers.

Autonomous Response blocks connections from the infected device, restricting its ability to scan the network and preventing malware from spreading further through the digital estate.

Potential unusual activity	Potential actions
› Unusual SMB enumeration › Suspicious Network Scan Activity › Unusual Network Scan › Unusual Admin SMB Session › Unusual Admin RDP Session › Unusual SSH › SMB Enumeration › Multiple Lateral Movement Model Breaches › Suspicious activity on high-risk device › Numeric Exe in SMB write › New or uncommon service control	✓ Block anomalous connections ✓ Enforce device pattern of life ✓ Enforce group pattern of life ✓ Quarantine devic

BRINGING THE HUMAN INTO THE LOOP

AI Analyst Investigations | Proactive Threat Notifications (PTN)

THIS ATTACK WOULD NOT HAVE PROGRESSED

4. DATA EXFILTRATION

1. Initiation | 2. Establish Foothold & Beaconing (C2) | 3. Lateral Movement | **4. Data Exfiltration** | 5. Data Encryption | 6. Ransom - $ | 7. Clean up & Recovery - $$$ | 8. The Cycle Repeats

Having established a strong foothold in the breached organization, the attacker begins to stage data in a central location prior to exfiltration. Data exfiltration elevates the breach to a double extortion ransomware attack.

As organizations insure against malicious encryption by becoming increasingly diligent with data backups, attackers have moved toward double extortion to secure their ransom payments. Exfiltrated data is used to blackmail organizations, with attackers threatening to publish sensitive information online or sell it on to the organization's competitors if they are not paid.

Data is exfiltrated with either a fast but conspicuous smash and grab approach, or a low and slow one which regularly exfiltrates small amounts of data over a period weeks or even months. Once it is complete, the same data can be encrypted within the organization's environment.

Legacy Security Solutions

Defenses that rely on either pre-programmed definitions of 'bad' or have rules constructed to combat different scenarios put organizations in a risky, never-ending game of cat and mouse.

Firewall & Proxy

A firewall and proxy might block connections based on pre-programmed policies based on specific endpoints or data volumes, but it's likely an attacker will live off the land and utilize a service that is generally allowed by the business, which might just include their own server which is unlikely to be blocked.

The effectiveness of these tools will vary according to data volumes: they might be effective for 'smash & grab' attacks, but are unlikely to spot low & slow exfiltration.

DLP

Might look at the packet level for sensitive predetermined corporate information/PII leaving the environment.

It might additionally prevent application-specific blocks, but businesses naturally create holes in their policies for legitimate business, enabling attackers to live off the land.

Might help for smash & grabs but is unlikely to detect low and slow exfiltration.

Darktrace's Autonomous Response

Working 24/7 at machine speed, Autonomous Response acts at the first indication of exfiltration, whenever it occurs.

Because it involves a break from expected behavior, even less conspicuous, low and slow data exfiltration is detected and stopped.

No confidential files are lost, and attackers are unable to extort a ransom payment through blackmail.

Potential unusual activity	Potential Actions
› Anomalous SMB › Uncommon 1 GiB outbound › Anomalous Download and Upload › Data sent to rare domain › Unusual External Data Transfer › Unusual data download to rare destination › Unusual data upload to rare destination	✓ Block anomalous connections ✓ Quarantine devices ✓ Enforce device pattern of life ✓ Enforce group pattern of life

BRINGING THE HUMAN INTO THE LOOP

AI Analyst Investigations | Proactive Threat Notifications (PTN)

THIS ATTACK WOULD NOT HAVE PROGRESSED

5. DATA ENCRYPTION

1. Initiation | 2. Establish Foothold & Beaconing (C2) | 3. Lateral Movement | 4. Data Exfiltration | **5. Data Encryption** | 6. Ransom - $ | 7. Clean up & Recovery - $$$ | 8. The Cycle Repeats

Encryption is the stage of the attack which grants the attacker the leverage they need in order to extort a ransom. Using either symmetric encryption, asymmetric encryption, or a combination of the two, attackers attempt to render as much data unusable in the organization's network as they can before the attack is detected.

As the attackers alone have access to the relevant decryption keys, they are now in total control of what happens to the organization's data.

Legacy Security Solutions

Firewall & Network Access Control (NAC)

Firewalls and NACs are unlikely to stop encryption without highly disruptive preprograming blocking off file servers in regular use by employees.

Typically, internal firewalls prevent clients from accessing servers, so once the attack has penetrated to servers it's essentially a free for all.

NIPS

Encryption falls outside of the scope of IDS or IPS tools, but a NIPS solution might see this traffic. To prevent encryption, this NIPS solution may have been pre-programmed to look for specific known suffixes in file rewrites but will struggle to detect novel ransomware or differentiate legitimate and malicious SMB usage. For example, differentiating ransomware and backups.

Endpoint Antivirus

Antivirus tools look only for known malware. If the malware has not been detected until this point, it is highly unlikely the antivirus will act here.

Darktrace's Autonomous Response

Even if familiar tools and methods are used to conduct it, Autonomous Response can enforce the normal pattern of life for devices attempting encryption, without using static rules or signatures. This action can be taken independently or via integrations with native security controls, maximizing the return on other security investments.

With a targeted Autonomous Response, normal business operations can continue while encryption is prevented.

Potential unusual activity	Potential Actions
› Additional extension appended to SMB file › Sustained MIME type conversion › Suspicious read write ratio › Possible Ransom Note › Suspicious SMB Activity	✓ Block anomalous connections ✓ Quarantine devices ✓ Enforce device pattern of life ✓ Enforce group pattern of life

BRINGING THE HUMAN INTO THE LOOP

AI Analyst Investigations | Proactive Threat Notifications (PTN)

THIS ATTACK WOULD NOT HAVE PROGRESSED

6. RANSOM - $

1. Initiation | 2. Establish Foothold & Beaconing (C2) | 3. Lateral Movement | 4. Data Exfiltration | 5. Data Encryption | **6. Ransom - $** | 7. Clean up & Recovery - $$$ | 8. The Cycle Repeats

This is where the malware gets its name.

A ransom note is deployed. The attackers request payment in return for a decryption key and threaten the release of sensitive exfiltrated data. The organization must decide whether to pay the ransom or lose their data, possibly to their competition or the public. The average demand made by ransomware threat actors rose in 2021 to **$5.3 million**, meat processing group JBS paying out $11 million and DarkSide receiving over $90 million in Bitcoin payments following the Colonial Pipeline incident.

Often, people believe their payment troubles are over at the ransom payment stage, but unfortunately, it's just beginning to scratch the surface.

7. CLEAN UP & RECOVERY - $$$

1. Initiation | 2. Establish Foothold & Beaconing (C2) | 3. Lateral Movement | 4. Data Exfiltration | 5. Data Encryption | 6. Random - $ | **7. Clean up & Recovery - $$$** | 8. The Cycle Repeats

The organization begins attempts to return its digital environment to order. Even if it has paid for a decryption key, many files may remain encrypted or corrupted.

Beyond the costs of the ransom payment, network shutdowns, business disruption, remediation efforts, and PR setbacks all incur hefty financial losses.

The victim organization may also suffer additional reputation costs, with **66%** of victims reporting a significant loss of revenue following a ransomware attack, and **32%** reporting losing C-level talent as a direct result from ransomware. With Darktrace's real-time detections and Autonomous Response at every stage of the attack, this can all be avoided. By understanding how your business behaves, Self-Learning AI stops ransomware at every stage and prevents cyber disruption.

Incident response

Efforts are made to try to secure the vulnerabilities which allowed the attack to happen initially – the organization should be conscious that approximately **80%** of ransomware victims will in fact be targeted again in the future.

Legacy tools largely fail to shed light on the vulnerabilities which allowed the initial breach. Like searching for a needle in an incomplete haystack, security teams will struggle to find useful information within the limited logs offered by Firewalls and IDSs. Antivirus solutions may reveal some known malware but fail to spot novel attack vectors.

With Darktrace's Cyber AI Analyst, organizations are given full visibility over every stage of the attack, across all coverage areas of their digital estate, taking the mystery out of ransomware attacks. They are also able to see the actions that would have been taken to halt the attack by Autonomous Response. The single thing the organization needs to ensure they are not one of the 80% of organizations who fall victim to ransomware again is made abundantly clear: Autonomous Response.

8. THE CYCLE REPEATS

1. Initiation | 2. Establish Foothold & Beaconing (C2) | 3. Lateral Movement | 4. Data Exfiltration | 5. Data Encryption | 6. Ransom - $ | 7. Clean up & Recovery - $$$ | **8. The Cycle Repeats**

Research shows that 80% of ransomware victims that pay the ransom suffer a second attack, often in the hands of the same group. The only way to truly keep the attackers from striking again is to know the full scope of the attack, ensure the attacker is no longer in your environment, and use a technology that doesn't look at connections and events on a one-off basis. Beyond taking precise and machine-speed action to contain ransomware at every stage, Darktrace AI assists with remediation following an attack, monitoring and containing additional suspicious behavior as devices come back online.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security AI, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. We protect more than 7,700 customers from the world's most complex threats, including ransomware, cloud, and SaaS attacks. Darktrace is delivering the first-ever Cyber AI Loop, fueling a continuous security capability that can autonomously spot and respond to novel in-progress threats within seconds. Darktrace was named one of TIME magazine's 'Most Influential Companies' in 2021.

To learn more, visit darktrace.com

Scan to LEARN MORE