## Stages of a Ransomware Attack

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.



## 2. Establish

1. INITIATION

3. Lateral 4. Data 5. Data 7. Clean up & Recovery - \$\$\$ 8. The Cycle Repeats Foothold & Beaconing (C2) 6. Ransom - \$ Encryption

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.

#### 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.

**Legacy Security Solutions** 

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.

If the initial breach is a simple, historical attack, it might

Secure Email Gateway

#### Malicious links Phishing (e.g. for credentials) and attachments Catch only when seen before **Firewall** O Requires configuration on a per-organization basis, often modified based on the needs of the business. O If the attack hits firewall where a rule or signature does not match it, it will bypass the firewall.

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

O Looks for known malware being downloaded,

leverages pre-programmed rules and uses

IDS/IPS

attack to have sufficiently similar traits to attacks that have been seen before.

O Looks at pre-defined patterns. Relies on a new

- 2. ESTABLISH FOOTHOLD & BEACONING (C2) 3. Lateral 4. Data 1. Initiation Exfiltration Movement

## tailored and precise, meaning no disruption is suffered

Darktrace's Autonomous Response

by the business. With Darktrace, ransomware attacks end here, but its Autonomous Response capabilities work at later stages as well. Secure Email Proportionate. Gateway progressive actions Darktrace constantly reassesses your Out of Character business and adjusts its

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

#### Suspicious Attachment

Suspicious link

- Solicitation Extortion
- Spoofing
- Network
- Unusual
- Incoming RDP
- Unusual file download
- Unusual .exe fileTorrenting

Al Analyst Investigations

At every stage, the Cyber

Al Analyst replicates the

human analyst's ability

narratives, surfacing

incidents.

5. Data

Encryption

At this stage, the attacker makes contact with the breached device(s), allowing them to control subsequent stages of

to piece together attack

and triaging significant

- IPs have never before been seen or used maliciously
  - ∅ Enforce pattern of life ⊗ Enforce group pattern of life

response based on new evidence and actions by

Convert or Strip

Attachment

⊗ Block specific

connections

IP xyz.xyz.xyz

E.g. Port 3389 to

Darktrace can deter-

mine which connec-

tions to block, even if

the port, protocol, or

an attacker.

- **BRINGING THE HUMAN INTO THE LOOP** 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.



6. Ransom - \$

Darktrace's Autonomous Response

allows normal business activity to continue.

7. Clean up & Recovery - \$\$\$

8. The Cycle

Repeats

Traditional defenses tend to be blind to Living off the Land Suspicious C2 connections and the downloads which tactics, whereby an attacker leverages existing, standard follow them are spotted, even when conducted using business practices to compromise an environment. regular programs or methods.

**Potential** Firewall & IDS/IPS unusual activity Potential actions These systems tend to look at connections in iso-⊗ Block specific Anomalous lation, rather than in the context of previous and connections connections potentially relevant connections, thereby making Connections to ∅ Enforce pattern of life E.g. as a device

## ment.

connections, allow downloads the legitimate, Beaconing activity to usual connections external rare endpoint to continue while quickly neutralizing

makes new

pattern of life

haven't done

E.g. Prevent this

device from doing anything its peers

Once they are detected as a threat, Autonomous Response halts these connections and downloads but

Unusual data download from rare destination Unusual data upload

Incoming remote

Al Analyst Investigations

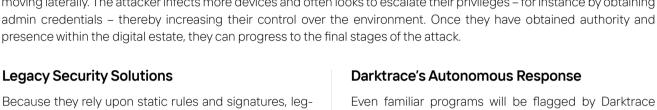
6. Ransom - \$

THIS ATTACK WOULD NOT HAVE PROGRESSED

8. The Cycle

7. Clean up &

**Proactive Threat** Notifications (PTN)



### 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 segmenta-

tion and a perfect configuration could prevent

a perfect balance between protective and disrup-

Because they rely upon static rules and signatures, leg-

acy solutions struggle to prevent lateral movement and

privilege escalation without also impeding essential busi-

ness operations. Novel methods of movement, including

**Legacy Security Solutions** 

3. LATERAL MOVEMENT

1. Initiation

2. Establish

Foothold &

Beaconing (C2)

IDS/IPS IPS denies network traffic when known threats are detected in packets, therefore requires the database to be constantly updated with new threats.

O 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.

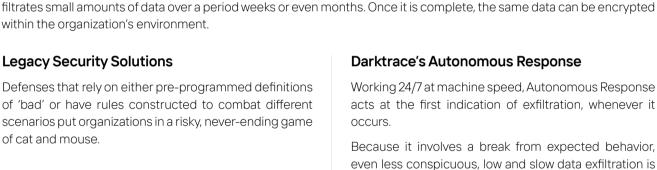
#### Unusual Admin **RDP Session** Unusual SSH SMB Enumeration

Multiple Lateral Movement Model Breaches Suspicious activity

BRINGING THE HUMAN INTO THE LOOP Al Analyst Proactive Threat

Notifications (PTN)

8. The Cycle



environment. BRINGING THE HUMAN INTO THE LOOP It might additionally prevent application-specific blocks, but businesses naturally create holes in their Al Analyst **Proactive Threat** Notifications (PTN) Investigations policies for legitimate business, enabling attackers to live off the land.

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.

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

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.

ransomware and backups.

**Endpoint Antivirus** 

6. RANSOM - \$

1. Initiation

1. Initiation

3. Lateral

4. Data

Exfiltration

4. Data

Exfiltration

2. Establish

Foothold & Beaconing (C2)

This is where the malware gets its name.

it's just beginning to scratch the surface.

7. CLEAN UP & RECOVERY - \$\$\$

The organization begins attempts to return its digital

environment to order. Even if it has paid for a decryption

Beyond the costs of the ransom payment, network

shutdowns, business disruption, remediation efforts,

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

key, many files may remain encrypted or corrupted.

and PR setbacks all incur hefty financial losses.

every stage and prevents cyber disruption.

3. Lateral

Movement

2. Establish

Beaconing (C2)

# 7. Clean up & Recovery - \$\$\$



Sustained MIME

type conversion

Suspicious read

Possible Ransom

Suspicious SMB

write ratio

Note

6. Ransom - \$

### 5. Data 6. Random - \$ Encryption

reveal some known malware but fail to spot novel attack

of organizations who fall victim to ransomware again is made abundantly clear: Autonomous Response. 7. Clean up & 5. Data 6. Ransom - \$

**Endpoint Antivirus** 

#### pre-programmed responses. • Rarely get deployed as they often do more harm than good, causing more disruption.

- 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

### Beacon to young any unusual events.

This is only possible SSL or HTTP when you understand beaconing to rare 'self' destination 

> to rare destinatio **BRINGING THE HUMAN INTO THE LOOP**



Autonomous Response blocks connections from the

infected device, restricting its ability to scan the network

and preventing malware from spreading further through

Potential actions

connections

∅ Enforce device

pattern of life

pattern of life

#### cross-network lateral movement. In reality, validating the efficacy of such a configuration is extremely difficult, however, and maintaining

tive controls near impossible.

response.

they are not paid.

of cat and mouse.

Firewall & Proxy

blocked.

within the organization's environment.

Legacy Security Solutions

 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 &

3. Lateral 1. Initiation Foothold & Beaconing (C2) Having established a strong foothold in the breached organization, the attacker begins to stage data in a central location

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

A firewall and proxy might block connections based

endpoints or data volumes, but it's likely an attacker

on pre-programmed policies based on specific

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

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

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

Might help for smash & grabs but is unlikely to

#### on high-risk device Numeric Exe in SMB write

Investigations

6. Ransom - \$

5. Data

Encryption

**Potential** 

unusual activity

Uncommon 1 GiB outbound

Anomalous Download

and Upload

domain

Data sent to rare

Unusual External

Data Transfer

Unusual data download to rare destination

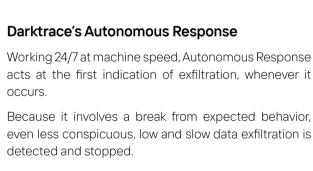
Anomalous SMB

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

Data is exfiltrated with either a fast but conspicuous smash and grab approach, or a low and slow one which regularly ex-

prior to exfiltration. Data exfiltration elevates the breach to a double extortion ransomware attack.

THIS ATTACK WOULD NOT HAVE PROGRESSED



## exfiltration. **DLP**

detect low and slow exfiltration.

organization's data.

**NIPS** 

**Legacy Security Solutions** 

5. DATA ENCRYPTION 2. Establish 3. Lateral 4. Data 1. Initiation Exfiltration Movement Beaconing (C2) Encryption is the stage of the attack which grants the attacker the leverage they need in order to extort a ransom.

## As the attackers alone have access to the relevant decryption keys, they are now in total control of what happens to the Darktrace's Autonomous Response

investments.

Activity BRINGING THE HUMAN INTO THE LOOP Al Analyst Proactive Threat Notifications (PTN) Investigations

> THIS ATTACK WOULD NOT HAVE PROGRESSED

# Often, people believe their payment troubles are over at the ransom payment stage, but unfortunately,

5. Data

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.

With Darktrace's Cyber Al 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%

#### 8. THE CYCLE REPEATS 2. Establish 3. Lateral 1. Initiation Foothold & Beaconing (C2)

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 Al assists with remediation following an attack, monitoring and containing additional suspicious behavior as devices come back online.

4. Data

DARKTRACE

Darktrace (DARK.L), a global leader in cyber security AI, delivers complete AI-powered solutions in its mission **About** to free the world of cyber disruption. We protect more than 7,700 customers from the world's most complex Darktrace threats, including ransomware, cloud, and SaaS attacks. Darktrace is delivering the first-ever Cyber Al 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

differentiation from normal traffic difficult. They may unusual endpoint block 'known-bad' domains or use some geo-block-Anomalous file ing, 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 endpoint rarity of the domain in the context of the environ-

desktop

- 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

5. Data

4. Data

**Potential** unusual activity **Unusual SMB** enumeration

Suspicious Network

Scan Activity

Network Scan

Unusual Admin

SMB Session

Unusual

if used maliciously by attackers.

the digital estate.

## New or uncommon service control

7. Clean up &

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

**Potential Actions** 

Quarantine devices

connections

∅ Enforce device

pattern of life

pattern of life

Unusual data upload to rare destination

THIS ATTACK WOULD

NOT HAVE PROGRESSED

## 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.

# Incident response

Legacy tools largely fail to shed light on the vulnerabilities

which allowed the initial breach. Like searching for a

static rules or signatures. This action can be taken independently or via integrations with native security controls, maximizing the return on other security With a targeted Autonomous Response, normal

∅ Enforce device

pattern of life

pattern of life

∅ Enforce group

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

business operations can continue while encryption is

8. The Cycle

Repeats

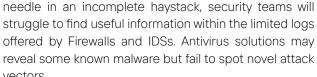
A ransom note is deployed. The attackers request payment in return for a decryption key and threaten the release of sensitive exfiltrated data. The organization must decide whether to pay the ransom or lose their data, possibly to their competition or the public. The average demand made by ransomware 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

7. Clean up & Recovery - \$\$\$

8. The Cycle Repeats

8. The Cycle

Repeats



info@darktrace.com

darktrace.com