THREATDOWN™

5 Early Signs of Ransomware

How to detect the initial stages of a ransomware attack

THREATDOWN™

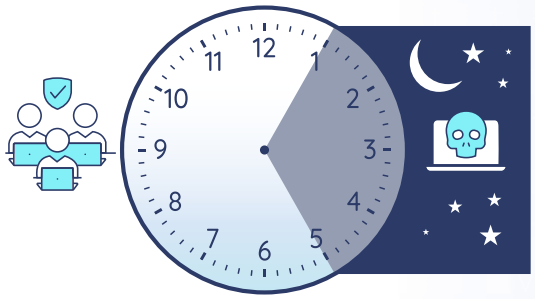
Contents

Why ransomware is getting harder to stop

Ransomware gangs have made considerable changes to their tactics over the past few years, to make them harder to stop. Attacks have gotten quicker, routinely happen at night, and increasingly rely on Living Off the Land (LOTL) techniques.

ThreatDown Malware Removal Specialists (MRS) have noted that ransomware gangs are increasingly launching attacks at night, particularly between 1 AM and 5 AM, when IT staff are likely to be asleep, and organizations will respond least quickly to security alerts.

Most ransomware attacks happen at night, between the hours of 1 A.M. and 5 A.M., while IT staff are more likely to be asleep

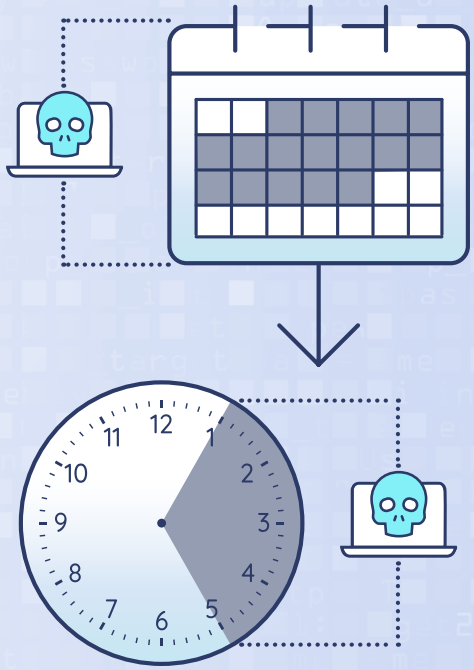


The speed of attacks has increased significantly too. ThreatDown Incident Response (IR) teams report that the time it takes to move through all the phases of an attack—from initial access through lateral movement, data exfiltration, and encryption—has shortened from weeks to hours.

Finally, the modern ransomware attack chain now relies heavily on LOTL techniques. Data from the ThreatDown Managed Detection & Response (MDR) team show that ransomware gangs are increasingly using legitimate software like remote desktops and system administration tools for malicious purposes.

With ransomware getting quicker and harder to detect, it has never been more important to catch attacks early.

What used to take weeks...



...now only takes hours.

THREATDOWN™

Knowing what to look for

Every ransomware attack starts with a breach triggered by something like a stolen credential, an exploited software vulnerability, or a malicious email attachment. In an ideal world, every phishing attempt would be blocked, every RDP port hardened, and every vulnerability patched—but in the real world that is not always the case.

So, while organizations should make every effort to prevent breaches, they must also prepare for some to be successful.

When a breach succeeds, ransomware gangs work through a series of steps to compromise an organization: privilege escalation, lateral movement, data theft, and then data encryption.

This guide to the early signs of ransomware covers the period between initial breach and data encryption: When ransomware gangs are working quietly inside an organization's network and endpoint detection and response (EDR) detects the subtle signs of their presence.

THREATDOWN™

#1: Identify password guessing attempts

Ransomware gangs love RDP for the same reason that regular users do: It provides the same access to a computer as walking into an office and sitting down in front of it, but from anywhere in the world. Consequently, there is an entire criminal industry devoted to guessing RDP passwords.

Detection systems that log multiple failed logins within a short time frame can signal that a ransomware gang is trying to find a way into a network.

Monitoring and responding to these attempts can prevent attackers from establishing a foothold.

Example IOCs:

1	**Multiple failed login attempts**	`Failed login from IP: 192.168.1.10, user: admin` `Failed login from IP: 192.168.1.10, user: admin` `Failed login from IP: 192.168.1.10, user: admin`

2	**Successful login after many failures**	`Failed login from IP: 192.168.1.10, user: admin`
		`Failed login from IP: 192.168.1.10, user: admin`
		`Successful login from IP: 192.168.1.10, user: admin`

3	**Frequent account lockouts**	`Account 'john.doe' locked due to 5 failed login attempts.`
4	**High amounts of traffic to login services (SSH, RDP, etc.).**	`Spike in SSH login attempts on port 22 from IP: 203.0.113.25`

THREATDOWN™

#2: Check known reconnaissance commands

Reconnaissance commands are used by ransomware gangs to gather information about a network they have breached and its users. Understanding the commands they use to gather information can therefore give defenders a significant advantage.

Often, ransomware gangs "live off the land" by using the same commands that network administrators use, such as `nltest`, `net user`, and `net group`. This makes it crucial that defenders understand not just which command was used, but who used it, when, and why.

EDR systems, such as ThreatDown EDR, often alert on reconnaissance commands.

.

Example IOCs:

1	**Nmap scanning**	**Command:** nmap -sS <target> **IOC:** Large amounts of SYN packets to various ports.
2	**Ping sweeps**	**Command:** ping <subnet> **IOC:** Increased ICMP traffic to multiple IP addresses.
3	**DNS Reconnaissance**	**Command:** nslookup <domain> or dig <domain> **IOC:** Unusual DNS queries, especially for internal domains.
4	**Active Directory Enumeration**	**Command:** SharpHound.exe (used in BloodHound AD recon) **IOC:** Large LDAP traffic or queries to AD domain controllers.

THREATDOWN™

#3: Spot out-of-place IT admin tools

Attackers often use legitimate IT admin tools to gain control over systems and perform malicious activities like data exfiltration. Because these tools do not look out of place, their use can easily go unnoticed. However, finding them in an unexpected location, such as an endpoint, can be an early indicator of a ransomware attack.

Recognizing IT admin tools and determining how recently they were created or installed on an endpoint are crucial.

Tools such as Remote Monitoring and Management (RMM) software, PsExec, Wireshark, and Advanced IP Scanner, if found unexpectedly, can signify an impending ransomware attack.

Example IOCs:

1	**Suspicious RMM activity**	**Event:** Unauthorized AnyDesk session initiated on domain-controller-01 **Source IP:** 198.51.100.50 (foreign IP) **Timestamp:** 3:22 AM **User:** LocalAdmin **Action:** Remote desktop control established
2	**Suspicious PowerShell activity**	**Event:** PowerShell script executed by user: marketing_user **Command:** powershell.exe -nop -w hidden -enc <obfuscated_base64_script> **Path:** C:\Users\marketing_user\AppData\Local\Temp\invoke-mimikatz.ps1 **Timestamp:** 1:45 AM **Action:** Extracting credentials using Invoke-Mimikatz
3	**Suspicious WMIC (Windows Management Instrumentation Command-line) activity**	**Event:** WMIC executed on HR-server-01 by user: guest_user **Command:** wmic process call create "cmd.exe /c whoami" **Source IP:** 203.0.113.15 **Timestamp:** 12:10 AM
4	**Suspicious PsExec activity**	**Event:** PsExec executed on finance-server-02 from IP: 192.168.1.100 **Command:** PsExec.exe \\finance-server-02 -u admin_user -p password cmd.exe /c "net user" **Timestamp:** 2:35 AM **Action:** Remote command execution for gathering user account info

THREATDOWN™

#4: Detect credential dumping

Ransomware gangs use a technique called credential dumping to acquire credentials from a compromised system, so that they can move laterally through a network and elevate their privileges.

Defenders can detect credential dumping by monitoring for unusual access patterns or the presence of applications like Mimikatz, a penetration-testing tool that can find and save authentication credentials such as Kerberos tickets.

Any unexpected or unauthorized attempt to access stored credentials should be investigated immediately.

Example IOCs:

1	**Access to LSASS process**	**Process:** procdump.exe targeting lsass.exe Source IP: 198.51.100.50 (foreign IP) **Path:** C:\Windows\System32\lsass.exe **Timestamp:** 11:15 PM **Action:** Memory dump saved as C:\Temp\lsass.dmp
2	**Credential dumping PowerShell commands**	**Command:** powershell.exe -nop -w hidden -enc dXNlciBpbmZvcm1hdGlvbg== **Path:** C:\Users\admin\AppData\Local\Temp\invoke-mimikatz.ps1 **Timestamp:** 2:30 AM **Action:** Obfuscated PowerShell script running to extract credentials from memory
3	**Access to sensitive files (ntds.dit, SAM)**	**File Access:** ntds.dit accessed on domain-controller-01 **Path:** C:\Windows\NTDS\ntds.dit **User:** guest_user (non-admin) **Timestamp:** 1:00 AM
4	**Execution credential dumping tools**	**Process:** Mimikatz.exe executed on HR-workstation-02 **Path:** C:\Users\HRuser\Downloads\Mimikatz.exe **Timestamp:** 3:00 AM **Action:** Credentials being dumped from lsass.exe

THREATDOWN™

#5: Close down backdoors

Backdoors are tools that allow attackers to reenter a network if their initial access is blocked, or if they are expelled from a compromised system.

Some backdoors even allow attackers to capture keystrokes or download additional payloads onto a target environment, and many ransomware gangs use backdoors like QBot or PikaBot, commonly delivered through malvertising.

Identifying and removing backdoors early can deprive ransomware gangs of access to a network.

Example IOCs:

1	**Unusual listening ports**	`Unknown service 'backdoor.exe' listening on port 4444.`
2	**Suspicious outbound connections**	`Outbound connection to suspicious IP 203.0.113.55 on port 8080.`
3	**Persistence via registry or scheduled tasks**	`Registry key created: HKLM\Software\Microsoft\Windows\Run\backdoor.exe.`
4	**Creation of new admin accounts**	`New admin account 'temp_admin' created at 2:15 AM.`

Spotting the five early signs

Using the five early signs to stop ransomware requires two things: The right tools, and the right people.

The right tools

Ransomware gangs work hard to stay hidden but their activity can be spotted by looking for patterns of suspicious activity. EDR is designed to pick up on suspicious activity and trigger alerts for things like password-guessing attempts, reconnaissance commands, out-of-place admin tools, credential dumping attempts, and backdoors.

ThreatDown EDR makes it easier to spot the five early signs by reducing the background noise of false positives and equips organizations to recover quickly from ransomware incidents by isolating affected machines and rolling back malicious encryption.

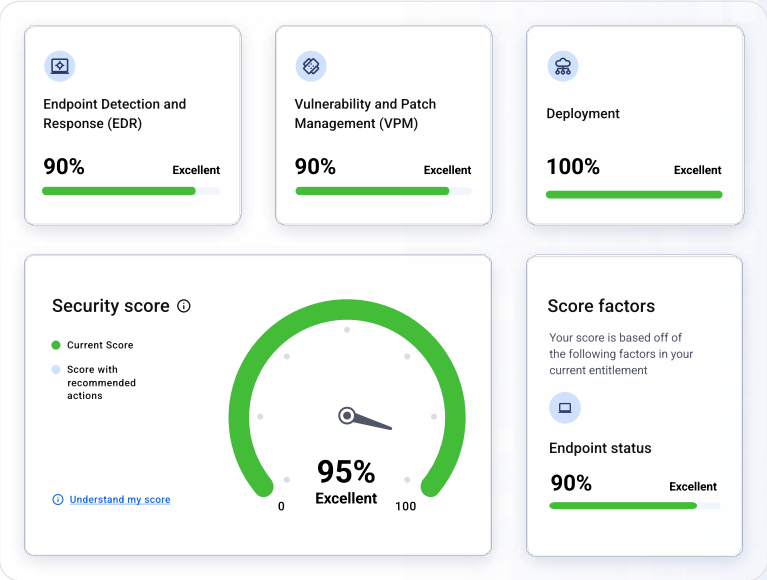
The right people

Ransomware gangs often operate at night, when they know IT staff are least likely to be watching. Managed detection and response (MDR) provides continuous EDR monitoring by security experts, 24 hours a day, so there is no time when ransomware gangs can operate unnoticed.

ThreatDown MDR is a global security operations center that monitors and investigates alerts day and night, staffed by threat hunters and incident responders with decades of combined experience investigating and mitigating complex threats.

THREATDOWN™

Protect against ransomware with ThreatDown MDR



ThreatDown MDR's always-on coverage is designed to deliver peace of mind and support business continuity at every turn.

- **24x7x365 monitoring**
  ThreatDown MDR watches your endpoints day and night, at weekends and through holidays.
- **Backed by SIEM and SOAR**
  Detection data is enriched and prioritized in real time to reduce noise and accelerate response times.
- **Powered by award-winning EDR**
  AI, machine learning, and heuristics technologies detect and interrupt payload delivery.

Get protected

THREATDOWN™ | threatdown.com | sales@threatdown.com