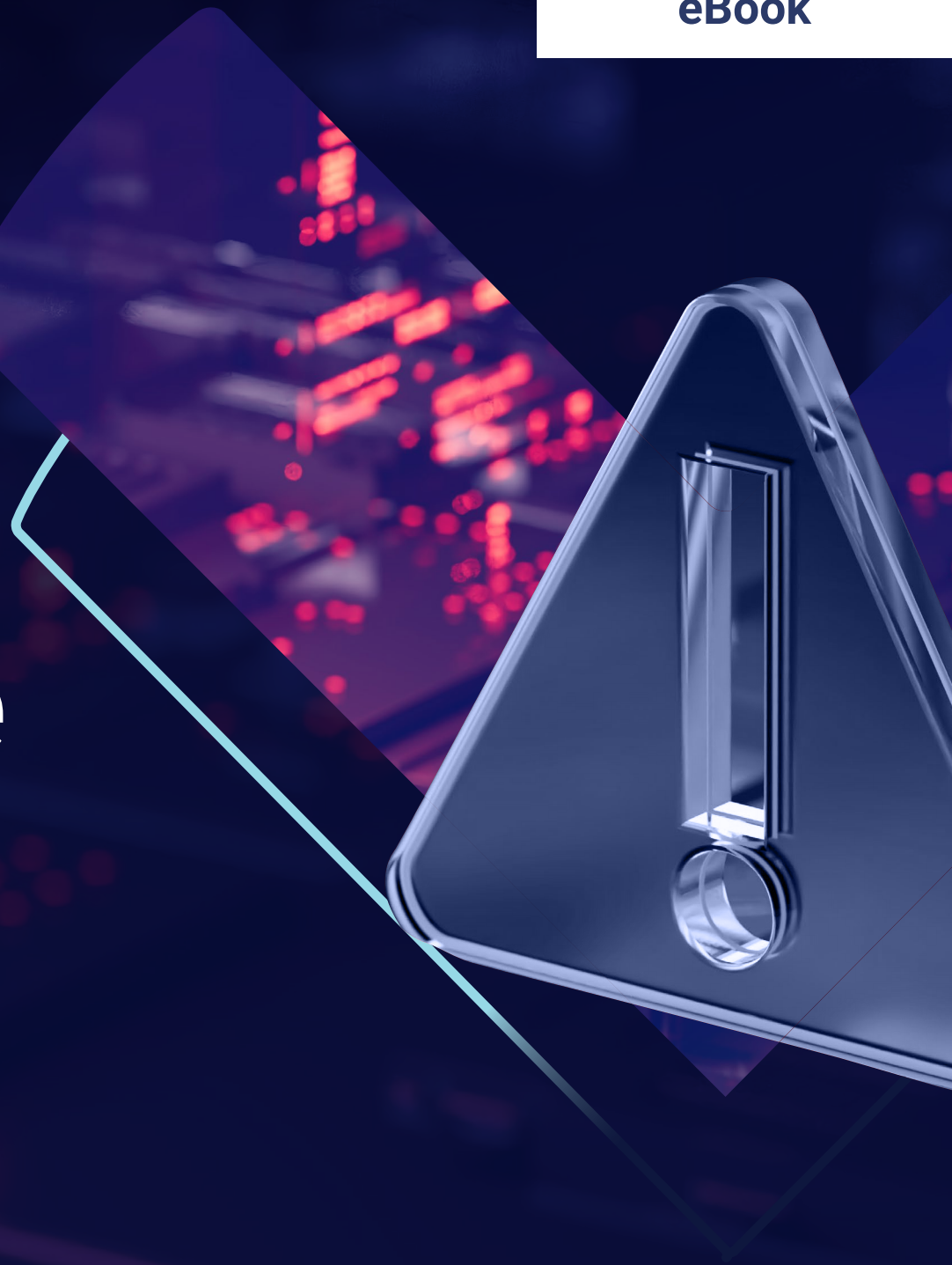
eBook

ThreatDown™
Powered by Malwarebytes



# Ransomware Cheat Codes

Shortcuts for winning the game against ransomware foes.

ThreatDown™ Powered by Malwarebytes

# Contents

**Ransomware is Quicker, Stealthier, and More After-Hours Than Ever** . . . . . 3

**How Ransomware Cheat Codes Can Help** . . . . . 4

**Cheat Code #1:** Check Brute Force Intrusion Detections . . . . . 5

**Cheat Code #2:** Know Reconnaissance Commands . . . . . 6

**Cheat Code #3:** Spot Out of Place IT Admin Tools . . . . . 7

**Cheat Code #4:** Detect Credential Dumping . . . . . 8

**Cheat Code #5:** Check for Backdoors . . . . . 9

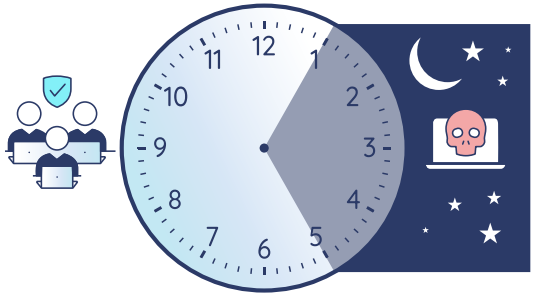
**Pressing Start On Your Cheat Code Journey** . . . . . 10

# Ransomware is Quicker, Stealthier, and More After-Hours Than Ever

**Ransomware gangs got a huge buff over the past year.**

For one, ransomware gangs are increasingly launching attacks during the night, particularly between 1 A.M. and 5 A.M., when IT staff are less likely to be monitoring systems. ThreatDown Malware Removal Specialists (MRS) have noted a surge in such early morning attacks over the past year.

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

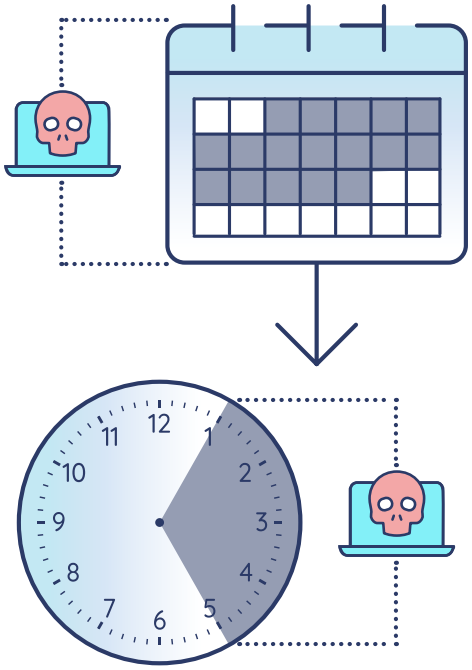


Second, the speed of attacks has drastically increased. The time required for ransomware gangs to execute an attack—from initial access through lateral movement, data exfiltration, and encryption—has shortened from weeks to mere hours, as observed by ThreatDown Incident Response (IR) teams.

Finally, there's a marked increase in the use of Living Off the Land (LOTL) techniques. Data from the ThreatDown Managed Detection & Response (MDR) team show that ransomware gangs are increasingly leveraging built-in system administration tools for malicious purposes. Incidents involving top gangs like LockBit, Akira, and Medusa reveal that much of the modern ransomware attack chain now heavily relies on LOTL techniques.

All of this is to say: If cybersecurity is a game, then it's safe to say that IT admins are playing it on hard mode right now. That's where cheat codes come in.

**What used to take weeks...**



**...now only takes hours.**

# How Ransomware Cheat Codes Can Help

**Just like how normal cheat codes help you gain an edge in video games, ransomware cheat codes help you gain an edge against ransomware attackers.**

How? By focusing on stopping ransomware gangs when it matters most—early on.

In an ideal world, stopping ransomware gangs early would happen at the prevention layer. For example, by successfully blocking every phishing attempt, closing (or hardening) every open RDP port, or patching every vulnerability in our environment.

But unfortunately, we don't live in an ideal world. It's always best to assume that an attack will eventually be successful. That way, we can be prepared for the worst case scenario.

Our cheat codes deal with the period right between initial access and encryption: When ransomware gangs are lurking in your systems and our EDR is picking up the subtle signs of their presence.

So while our cheat codes won't give you an infinite supply of money like they might in some other games, they will help you stop an ongoing ransomware attack early on—which is sort of a payday of its own.

**Let's dive into it.**

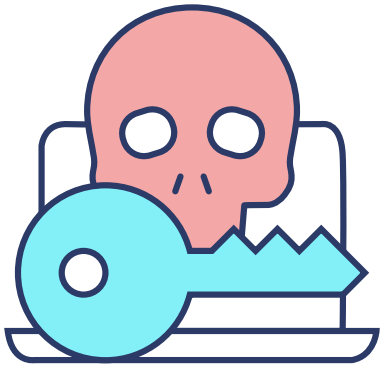
ThreatDown Powered by Malwarebytes

# **Cheat Code #1:** Check Brute Force Intrusion Detections

If someone shows up to your castle with a battering ram and starts hammering away at the front gate, it's a pretty good sign that something bad is about to happen.

The same is true for brute force attacks, when threat actors repeatedly attempt to gain access to a system by guessing passwords: Detection systems that log multiple failed login attempts, especially within a short time frame, can signal that a ransomware gang is trying to force its way in your network.

Monitoring and responding to brute force intrusion detections can prevent attackers from establishing a foothold in a network.



## IOCs to look for:

1. **Multiple failed login attempts**

   **Example:**

   ```
   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**

   **Example:**

   ```
   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**

   **Example:**

   ```
   Account 'john.doe' locked due
   to 5 failed login attempts.
   ```

4. **High amounts of traffic to login services (SSH, RDP, etc.).**

   **Example:**

   ```
   Spike in SSH login attempts on
   port 22 from IP: 203.0.113.25
   ```

# **Cheat Code #2:** Know Reconnaissance Commands

You're a ninja in a video game tasked with breaking into the king's castle. Sounds good, but without a map of the place, you have no idea where everything is—including the gold coins you're after.

Maps are also one of the first things ransomware gangs are looking for when they break into your network. If your EDR picks up any reconnaissance commands being used, it could mean a ransomware gang is searching for 'maps' of your network.

Reconnaissance commands are used by ransomware attackers to gather information about a network and its users. EDR systems, such as ThreatDown EDR, often alert on reconnaissance-type commands such as `nltest, net user, and net group`. While these commands can be benign, their context is critical—making them a perfect example of a Living off the Land (LOTL) technique.

IT administrators must verify if they recognize the commands run for the user account on the endpoint, the time they were executed, and whether they align with regular administrative activities.

## IOCs to look for:

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 Powered by Malwarebytes

# **Cheat Code #3:** Spot Out of Place IT Admin Tools

It goes without saying that the quicker you find the imposter in Among Us, the faster you can win the game. The same is true when it comes to finding an attackers' IT admin tools on an endpoint, which can be an early indicator of a ransomware attack.

Attackers use IT admin tools to gain control over systems and perform various malicious activities such as data exfiltration—and because these tools are legitimate, they're all the more hard to spot.

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

## IOCs to look for:

1. **Suspicious RMM activity**

   **Example:**

   **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**

   **Example:**

   **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**

   **Example:**

   **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**

   **Example:**

   **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 Powered by Malwarebytes

# **Cheat Code #4:** Detect Credential Dumping

Whether it's for work or our favorite game, our login info is everything—and if we can detect someone in the act of trying to steal that info, we can stop an ongoing attack.

Ransomware attackers are always on the lookout for your login info with a technique called credential dumping, which involves extracting account login credentials from a compromised system. Attackers use these credentials to move laterally within a network and escalate privileges.

Monitoring for unusual access patterns or the presence of tools like Mimikatz, which is commonly used for credential dumping, can help identify a ransomware attack in the early stages. Any unexpected or unauthorized attempt to access stored credentials should be investigated immediately.

## IOCs to look for:

1. **Access to LSASS process**

   **Example:**

   **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**

   **Example:**

   **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)**

   **Example:**

   **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 of known credential dumping tools**

   **Example:**

   **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

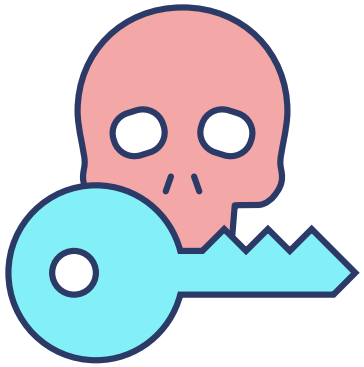
ThreatDown Powered by Malwarebytes

# **Cheat Code #5:** Check for Backdoors

When you die in a video game, you usually respawn—backdoors allow an attacker to essentially do the same, giving them reentry into a system even after they've been kicked out.

Some backdoors even allow attackers to capture keystrokes or download additional payloads in the victim environment, and many ransomware gangs use multipurpose backdoors like QBot or PikaBot, commonly delivered through malvertising.

All of which is to say: If you can spot (and remove) any backdoors on your systems early, you can deprive ransomware gangs of a significant tool in their attack arsenal.



## IOCs to look for:

1. **Unusual listening ports**

   **Example:**

   ```
   Unknown service 'backdoor.exe'
   listening on port 4444.
   ```

2. **Suspicious outbound connections**

   **Example:**

   ```
   Outbound connection to
   suspicious IP 203.0.113.55 on
   port 8080.
   ```

3. **Persistence via registry or scheduled tasks**

   **Example:**

   ```
   Registry key created: HKLM\
   Software\Microsoft\Windows\Run\
   backdoor.exe.
   ```

4. **Creation of new admin accounts**

   **Example:**

   ```
   New admin account 'temp_admin'
   created at 2:15 AM.
   ```

# Pressing Start On Your Cheat Code Journey

Ransomware might be quicker, stealthier, and more after-hours than ever, but with these five cheat codes, you're well on the path to winning the game against ransomware foes. But how can you actually deploy them?

Well, it all starts with having the right tools in place.

To detect brute force attacks, LOTL techniques, and credential dumping, for example, you'll need an EDR that's configured to pick up on suspicious activity and trigger alerts when something's not right. The key point here, however, is to not just set it and forget it—focus on proper configuration, especially when it comes to access management and the principle of least privilege.

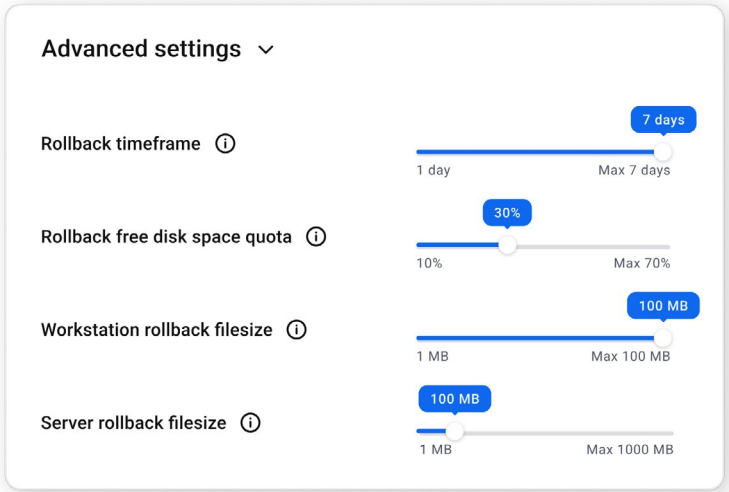
Having a top-tier EDR generating suspicious alerts is one thing, but it's only half the battle. Without skilled players actively monitoring those alerts, they're just noise.

To truly stay ahead of ransomware threats, you need continuous monitoring by experts who know what to look for and how to act swiftly. Whether through an in-house team or a managed detection & response (MDR) service, having the right people in place ensures that when an alert goes off, there's someone ready to jump in, investigate, and neutralize the threat before it spirals out of control.

It's not just about having the right tools—it's about having the right team to wield them effectively.

In summary, deploying these cheat codes means combining cutting-edge technology with expert oversight, ensuring you're ready to tackle ransomware threats head-on—no matter when they strike.

# Prevent, Protect, and Remediate Ransomware with ThreatDown




**Stay ahead of ransomware threats with ThreatDown. We combine the power of EDR and MDR for end-to-end protection, including:**

- **Ransomware Rollback**
  Return devices to a healthy state by undoing file and configuration changes.
- **Next-Gen Antivirus**
  Prevent threats from infiltrating your environment.
- **Anytime Access to a Security Expert**
  Answer questions, discuss remediation steps, and verify suspicious activity.

**Get protected**

ThreatDown™ Powered by Malwarebytes | threatdown.com | sales@threatdown.com