ThreatDown™
Powered by Malwarebytes

Threat Brief: Ransomware Gangs & Living Off the Land Attacks

November 2023

INTRODUCTION

Over the past year especially, organizations of all sizes have felt the scourge of Ransomware-as-a-Service (RaaS) gangs. Just consider that, from July 2022 to June 2023, there were 1,900 total ransomware attacks in just four countries—the US, Germany, France, and the UK.

To combat the pervasive ransomware threat, organizations should be aware of one of the most common techniques gangs use to evade detection and steal data: **Living Off The Land (LOTL).**

LOTL attacks are when attackers leverage legitimate tools to perform malicious actions. By mimicking normal behavior, LOTL attacks make it extremely difficult for IT teams and security solutions to detect any signs of malicious activities.

In this threat brief, we'll look more closely at the intersection of RaaS gangs and LOTL attacks, including LOTL tools commonly used by top gangs like LockBit, how LOTL techniques fit into a typical ransomware attack chain, and a real example of what it's like to battle a LOTL attack on the front-lines.

> *LOTL attacks represent a sophisticated evolution in strategies employed by RaaS gangs. By leveraging legitimate tools and processes, these threat actors can effectively 'hide in plain sight,' challenging their detection and mitigation. This underscores the need for robust security strategies, multi-layered security measures, and continuous network monitoring to promptly identify and respond to such stealthy tactics.*

Marcelo Rivero
Senior Malware Research Engineer,
Research & Response
Malwarebytes

COMMON TOOLS EXPLOITED BY RAAS GANGS

TOOL	USED FOR	USED TO	USED BY
PowerShell	Versatile scripting language and shell framework for Windows systems	Execute malicious scripts, maintain persistence, and evade detection	LockBit, Vice Society, Royal, BianLian, ALPHV, Black Basta
PsExec	Lightweight command-line tool for executing processes on remote systems	Execute commands or payloads via a temporary Windows service	LockBit, Royal, ALPHV, Play, BlackByte
WMI	Admin feature for accessing and managing Windows system components	Execute malicious commands and payloads remotely	LockBit, Vice Society, Black Basta, Dark Power, ClOp, BianLian
Cobalt Strike	Commercial penetration testing framework used to assess network security by mimicking an advanced attacker after initial compromise	Command and control, lateral movement, and exfiltration of sensitive data	LockBit, Black Basta, Royal, ALPHV, Play, Cuba, Vice Society

LOTL BROKEN DOWN BY THE EXPERTS

Hiep Hinh

Hiep Hinh is a Principal MDR Analyst at Malwarebytes, where he supports ThreatDown MDR 24/7/365 managed detection and response for customers around the globe. Hiep has over 16 years of experience in the cybersecurity and intelligence fields, including for the US Army as an intelligence analyst and for the Air Force Computer Emergency Response Team (AFCERT/33NWS).

> *For effective detection of LOTL attacks, understanding the environment is paramount. This requires knowledge of typical network activities, such as standard user behaviors, their usual online hours, and common data usage patterns. Armed with this baseline, security analysts can then identify anomalies or outliers, such as users active at unusual times or those using tools like command interfaces and PowerShell, which might not be inherently malicious but are uncommon for the environment.*

Shawn Dorsey

Shawn Dorsey is a Senior Director of Global Managed Services at Malwarebytes, where he leads the talented group of ThreatDown MDR analysts day-to-day. In his over 20 years of cybersecurity experience, Shawn has worked as a Special Agent for the Naval Criminal Investigative Service (NCIS) and has helped spearhead incident response efforts at companies such as Sony, Symantec, and Accenture.

> *Unless there's regular auditing or another trigger for investigation, detecting LOTL is challenging. It's like a person in a conspicuous outfit trying to break into an office versus a person walking in dressed in business attire. While the former instantly raises alarms, the latter may go unnoticed unless specifically scrutinized. APT groups favor this approach because of its discretion, allowing them to remain undetected in networks for extended periods, sometimes even years. The longest I've seen was a staggering seven years.*

LOTL TECHNIQUES IN THE RANSOMWARE ATTACK CHAIN

In the ransomware action chain, data exfiltration and encryption are just the final acts of a long-drawn series of malicious activities. Before the final payload can be delivered, ransomware gangs have to execute commands, download malicious scripts, and move laterally within a network—all of which they rely on legitimate programs to accomplish.

Let's look at the #1 most active ransomware gang in 2023, LockBit, as an example.

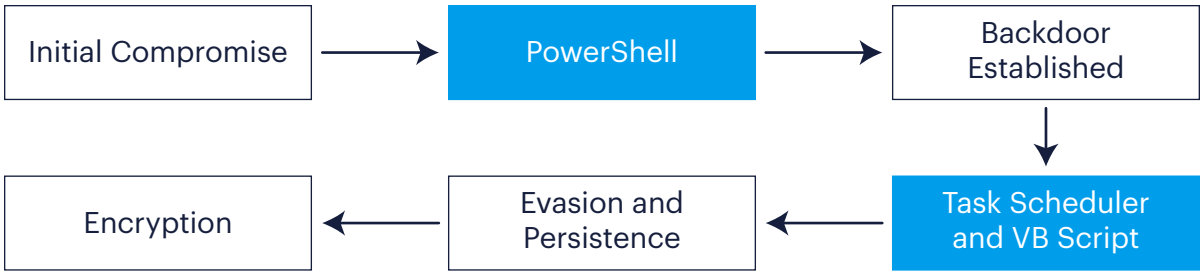


Figure 1: Sample LockBit attack chain

As you can see in the flowchart above, LockBit jumps into using LOTL techniques immediately after initial compromise. In this case, the LockBit uses PowerShell—a versatile and legitimate scripting tool for Windows systems—to retrieve encoded scripts from Google Sheets. These scripts create a persistent backdoor on the infected system, ultimately helping LockBit perform reconnaissance and disable some anti-malware capabilities on the targeted system.

Another LOTL technique comes into play when LockBit uses the Task Scheduler—a genuine Windows service—to set tasks that execute malicious VB Scripts at specific times or intervals. These scripts help LockBit maintain a foothold in the compromised system and ensure their malicious activities continue even after system reboots or user logins.

Let's look at more examples from two other highly-active ransomware gangs in 2023, ALPHV and Royal.

Figure 2: Sample ALPHV attack chain

In their ransomware attacks, ALPHV is known to employ the Microsoft Sysinternals suite, notably tools like PsExec, to execute commands remotely on systems and aid in lateral movement. Like LockBit, ALPHV also uses Windows Task Scheduler to configure malicious Group Policy Objects (GPOs) to deploy ransomware and turn off security features within the victim's network.

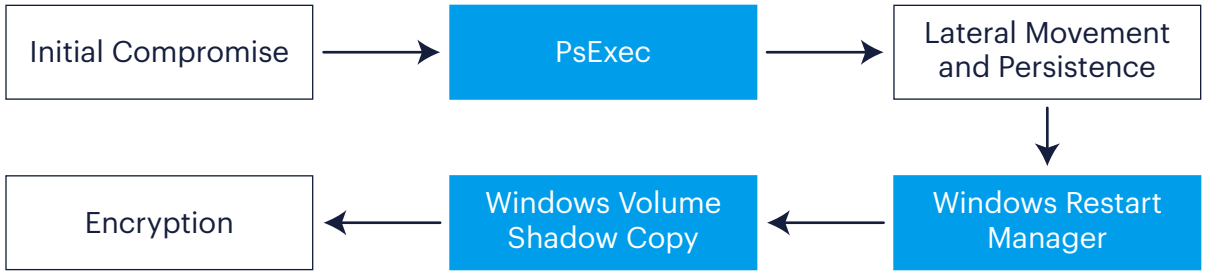


Figure 3: Sample Royal attack chain

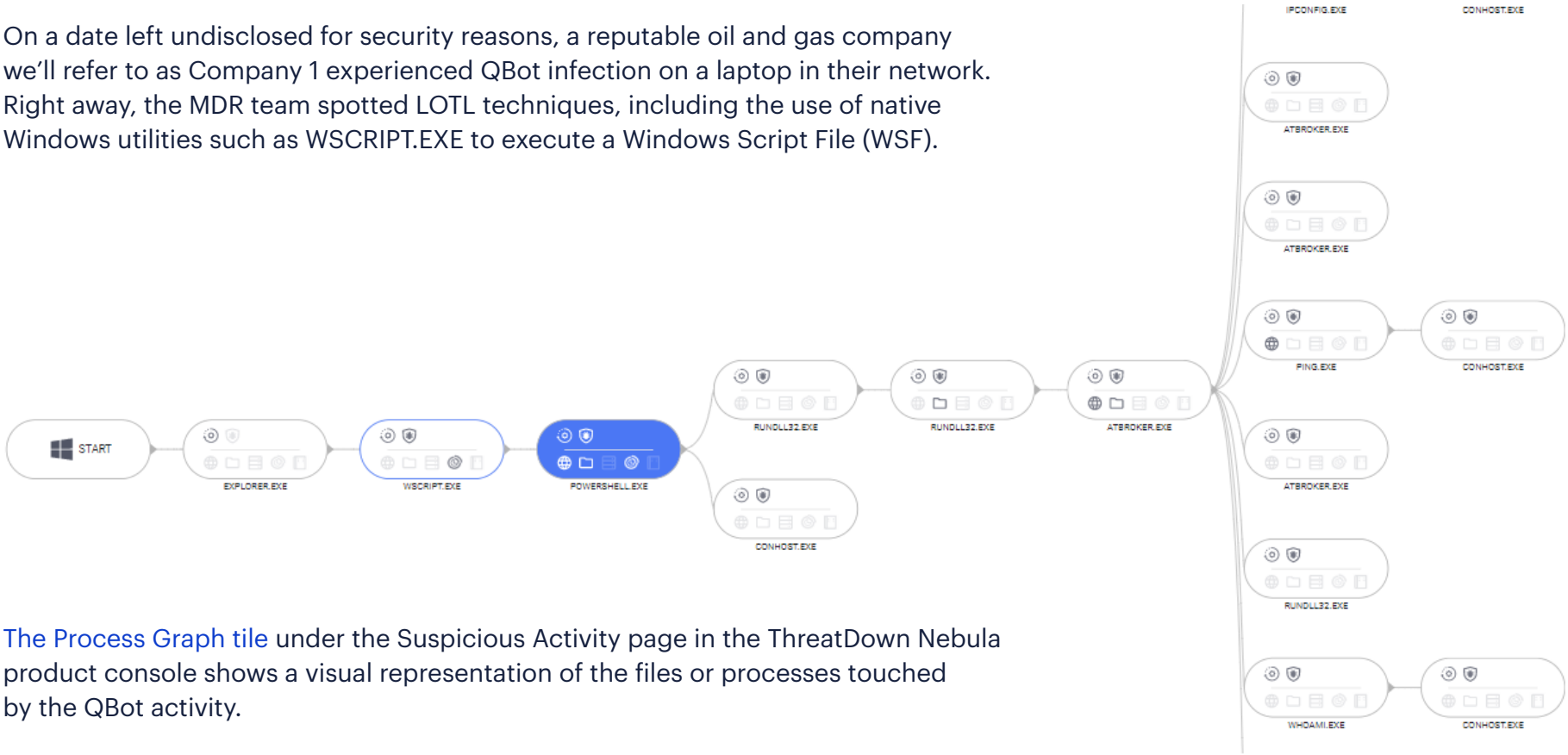
The Royal ransomware group has also been seen exploiting PsExec to aid lateral movement. Additionally, Royal uses the Windows Restart Manager before encryption to determine whether targeted files are currently in use or blocked by other applications. Another LOTL tool in their arsenal is Windows Volume Shadow Copy service, which they deploy to delete shadow copies of files, preventing system recovery efforts.

In summary, the deep integration of ransomware operations within standard Windows functionalities makes RaaS activities particularly elusive. The real challenge for defenders, then, lies in differentiating these camouflaged actions from regular administrative tasks.

AN MDR WAR STORY: BATTLING LOTL ATTACKS ON THE FRONT-LINES

Let's examine a time where the ThreatDown MDR team spotted the LOTL techniques of QakBot (QBot), a versatile banking trojan used by the Royal ransomware gang to maintain persistence on a compromised systems. **Note: While Qbot was taken down by the FBI in late August, remember ransomware operators remain active and will pivot to using LOTL techniques with new malware.**

On a date left undisclosed for security reasons, a reputable oil and gas company we'll refer to as Company 1 experienced QBot infection on a laptop in their network. Right away, the MDR team spotted LOTL techniques, including the use of native Windows utilities such as WSCRIPT.EXE to execute a Windows Script File (WSF).



The Process Graph tile under the Suspicious Activity page in the ThreatDown Nebula product console shows a visual representation of the files or processes touched by the QBot activity.

User Account:
COMPANY\[redacted]

Path:
C:\WINDOWS\SYSTEM32\WSCRIPT.EXE

PID:
9604

PID Version:
0

Hashes:
MD5: 0639b0a6f69b3265c1e42227d650b7d1
SHA1: 545ec11dee642de633eb2c6f6ffc90cce4decf8d
SHA256: ce9f70e104c07d92fc05fbd6000839fd6a87ff010e706396f87dd679244ed97b

Relation:
Create Process

Activities:
Antimalware Scan: 1

Command Line:
"C:\WINDOWS\System32\WScript.exe" "C:\Users\[redacted]\AppData\Local\Temp\Temp1_ujp (1).zip\DCEDc0OZCr7UmgfyPCLKb1bePSmvat8ba2uepd5REp.wsf"

Clicking on the node to view more details, the MDR team saw that WSCRIPT.EXE was used to execute a Windows Script File (WSF), which spawned an instance of PS executing a Base64 encoded command. By using native Windows utilities in this manner, attackers tried to make sure their actions didn't raise immediate suspicion.

Another node detail above shows malicious encoded PowerShell script. Spawning PowerShell from a script (like a WSF) provides another layer of obfuscation, complicating detection.

This script was designed to be patient and stealthy. It first initiated a waiting period of 4 seconds before creating an array of URLs, presumably leading to malicious websites. The malware then attempted to download a file from each URL. The downloaded files were executed using the legitimate RUNDLL32.EXE Windows utility, which was invoked from the PowerShell instance.

Path:
C:\WINDOWS\SYSTEM32\WINDOW...OWERSHELL.EXE

PID:
16728

PID Version:
0

Hashes:
MD5: f8278db78be164632c57002e82b07813
SHA1: ec824ee03f969721aef5ac2a7d5897d5d150cb13
SHA256: 9af8a2d9ca5d904b9ca6696016b2a794ef7eb97693ccca22df2a367305d31b88

Relation:
Create Process

Activities:
File Write: 5
Net Connect Outbound: 1
Antimalware Scan: 2
File Delete: 2

Command Line:
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC "UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANAA7ACQAUA...AYQByAHQALQBTAGwAZQBlAHAAIAAtAFMAZQBjAG8AbgBkAHMAIAA0ADsAfQB9AA==="

At this point, the stage was perfectly set for a ransomware gang like Royal to take things a notch higher.

After securing an initial foothold via the QBot infection and ensuring stealthy persistence using LOTL techniques, the Royal gang could have proceeded with enhanced reconnaissance, lateral movement, or pre-encryption tactics like disabling backup processes.

However, the Malwarebytes MDR team promptly detected the LOTL activities of QBot and quickly contained the infection, taking steps such as cleaning the system of the infection, informing Company 1 of the incident, and providing actionable recommendations to prevent future compromises.

ADVICE FOR I.T. TEAMS

The four tips listed below, combined with cutting-edge technology and unique expertise, can greatly help IT teams uncover LOTL attacks from RaaS gangs:

1. Regularly monitor network traffic and logs

Regularly analyze your network traffic for any unusual patterns or connections to known malicious IP addresses or domains associated with the use of tools like Chisel, Qakbot, or Cobalt Strike.

Enable logging on critical systems (firewalls, servers, and endpoint devices) and regularly review logs for unusual activities or signs of compromise.

2. Stay informed of the latest threat intelligence

Leverage threat intelligence feeds to stay informed about new attack techniques, indicators of compromise (IOCs), and other relevant threat data.

Use this data to fine-tune your security monitoring, detection, and response capabilities to identify and mitigate LOTL attacks.

3. Leverage behavioral analysis and anomaly detection

Implement advanced monitoring solutions that focus on detecting unusual user or system behavior rather than relying solely on known signatures or patterns.

Machine learning and artificial intelligence can be leveraged to identify deviations from normal behavior, which might indicate an ongoing LOTL attack.

ThreatDown EDR observes the behaviors of processes, registry, file system, and network activity on the endpoint using a heuristic algorithm looking for deviations. Here you can see all detection rules triggered in the suspicious activity and their mapping to MITRE ATT&CK.

4. Restrict the abuse of legitimate tools

Focus on managing and controlling the use of legitimate tools and system features often exploited in LOTL attacks.

Limit access to certain tools only to users who require them, monitoring their usage, and applying specific security policies to restrict potentially harmful actions.

CONCLUSION

In short, by continuously analyzing network and system data, identifying potential weak points, and anticipating attacker tactics, IT teams can begin to get the upper-hand against RaaS gangs that employ LOTL techniques.

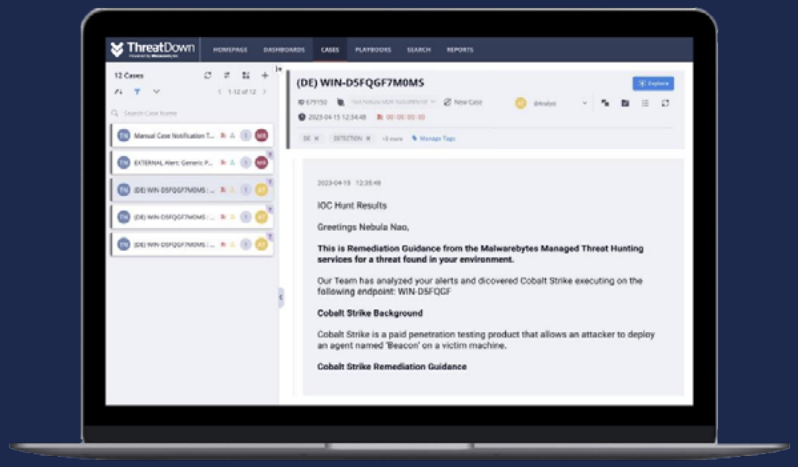
However, monitoring network traffic and checking for anomalies often requires around-the-clock coverage and deep cybersecurity expertise, which can be difficult for small and medium-sized organizations to maintain.

That's where ThreatDown Managed Detection and Response (MDR) comes in.

ThreatDown MDR analysts are experienced in detecting malicious use of legitimate tools and blocking attackers. They use their expertise to identify unusual patterns or connections to malicious IP addresses, domains, or unauthorized application usage related to the LOTL attacks conducted by the RaaS gangs.

ThreatDown
Managed Detection & Response

The best of both technology innovations and human expertise



- **24x7x365 threat monitoring** by Malwarebytes security experts
- **Proactive threat hunting** to limit future threats and exposure
- **Rapid response** to expedite recovery and reduce downtime

Get a quote

ThreatDown™ Powered by Malwarebytes | www.malwarebytes.com/business | corporate-sales@malwarebytes.com | 1.800.520.2796