

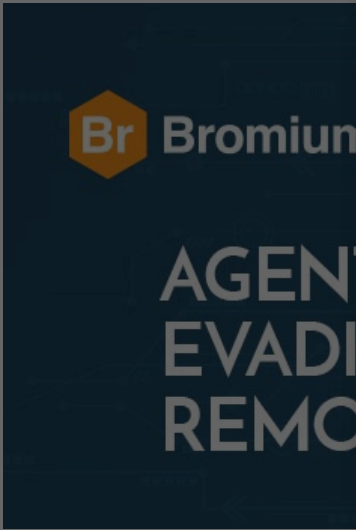


[Home](#) » [Security Bloggers Network](#) » Agent Tesla: Evading EDR by Removing API Hooks



Agent Tesla: Evading EDR by Removing API Hooks

[by Ratnesh Pandey](#) on August 11, 2019






Written by Toby Gray and Ratnesh Pandey

Endpoint detection and response (EDR) tools are designed to detect and respond to malicious activity that is generated by malware. These tools typically rely on analyzing system logs and application program interface (API) calls to detect anomalous behavior. We recently came across a phishing campaign that used a custom-built Trojan. While analysing the forensic data, we noticed several memory tampering events in the address space of ntdll.dll, the dynamic-link library (DLL) that exports the Windows Native API. The payload was isolated by Bromium Secure Platform and captured the malware.

The Agent Tesla downloader arrived as a .xls file which drops and executes the primary payload. In this blog post we cover the unhooking of APIs by the dropper to evade detection by tools such as EDR that rely on hooking. In a subsequent blog post, we provide an in-depth analysis of the campaign.



Security Boulevard asks for your consent to use your personal data to:

-  Personalised advertising and content, advertising and content measurement, audience research and services development
-  Store and/or access information on a device
-  Learn more

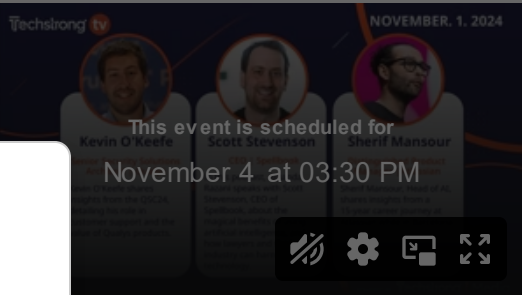
Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.

[Do not consent](#) [Consent](#)

[Manage options](#)

Techstrong TV



[Click full-screen to enable volume control](#)
[Watch latest episodes and shows](#)

Field Day Showcase



Upcoming Webinars



Podcast



[Listen to all of our podcasts](#)

Press Releases



***The Impact and
Utility of User Security
Data in Web3***

GoPlus’s Latest Report Highlights How Blockchain Communities Are Leveraging Critical API Security Data To Mitigate Web3 Threats

System Calls

A system call is a function in the kernel of an operating system that services requests from users and provides a barrier so that underlying high-privilege resources cannot be directly accessed by the user. On Windows systems, the ntdll.dll library contains user mode system calls. Information about these system calls are stored in an array of function pointers and the System Service Descriptor Table (SSDT).

```
//  
// System Service Table Descriptor  
//  
typedef struct _KSERVICE_DESCRIPTOR_TABLE  
{  
    PULONG_PTR Base;  
    PULONG Count;  
    ULONG Limit;  
    #if defined(_IA64_)  
        LONG TableBaseGpOffset;  
    #endif  
    PCHAR Number;  
} KSERVICE_DESCRIPTOR_TABLE;
```

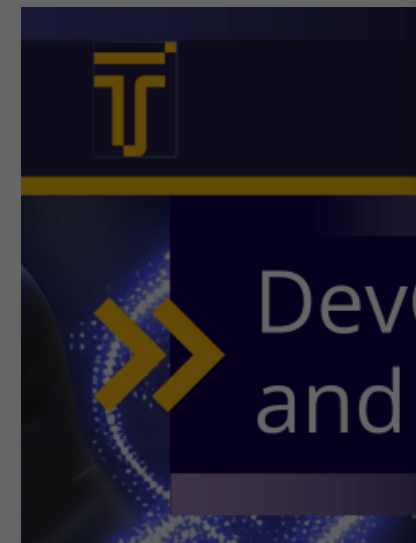


Figure 1 – The SERVICE_DESCRIPTOR_TABLE structure and system calls.



The “Base” points to the function pointer array and the system call number is an index into this array. These functions are used to request the kernel to perform some action, such as allocating virtual memory in the case of [NtAllocateVirtualMemory](#). For the rest of this discussion we’ll focus on NtProtectVirtualMemory, which is an undocumented system call that’s used to change the permissions of memory.

32-bit code on 64-bit Windows

When a 32-bit program is run on a 64-bit Windows machine, it runs under a system known as Windows on Windows 64 (or WoW64 for short). Because the kernel is running in 64-bit mode, system calls from 32-bit programs all go via a wrapper function, Wow64SystemServiceCall, which is at a known location in memory. This means that ntdll.dll, which contains many system call functions, has a very repetitive structure:



Security Boulevard asks for your consent to use your personal data to:

-  Personalised advertising and content, advertising and content measurement, audience research and services development
-  Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.



Subscribe to our Newsletters

Get breaking news, free eBooks and upcoming events delivered to your inbox.

Enter your email address*

View Security Boulevard [Privacy Policy](#).

Subscribe Now

• 77BAE20E	C2 0000	ret	14	
• 77BAE20F	90	nop		
• 77BAE210	B8 50000000	mov	eax,50	NtProtectVirtualMemory
• 77BAE215	BA 30248C77	mov	edx,ntd11.77BC2430	
• 77BAE21A	FFD2	call	edx	
• 77BAE21C	C2 1400	ret	14	
• 77BAE21F	90	nop		
• 77BAE220	B8 51000000	mov	eax,51	ZwQuerySection
• 77BAE225	BA 30248C77	mov	edx,ntd11.77BC2430	
• 77BAE22A	FFD2	call	edx	
• 77BAE22C	C2 1400	ret	14	

Figure 2 – Disassembly of NtProtectVirtualMemory.

The four lines of the disassembly code of NtProtectVirtualMemory are broken down as:

- Load the system call number 0x50 into the eax register
- Put the location of Wow64Transition (0x77BC2430 in the above screenshot) into the edx register
- Call the function at edx
- Return from this function

The next system call function, ZwQuerySection, is immediately after this one and follows the same structure, the only difference being loading 0x51 as the system call number rather than 0x50.

Hooking APIs

Security products use API hooking to intercept and record system API calls from software. One way of accomplishing this is to hook the API call.

When hooked, the first instruction of the hooked function is replaced with the code generated by the hooking process.

• 77BAE200	B8 4F000800		
• 77BAE205	BA 30248C77		
• 77BAE20A	FFD2		
• 77BAE20C	C2 0800		
• 77BAE20F	90		
• 77BAE210	E9 FD1D9488		
• 77BAE215	BA 30248C77		
• 77BAE21A	FFD2		
• 77BAE21C	C2 1400		
• 77BAE21F	90		
• 77BAE220	B8 51000000		
• 77BAE225	BA 30248C77		
• 77BAE22A	FFD2		
• 77BAE22C	C2 1400		

Figure 3 – Original function

In figure 3, the first instruction of the hooked function is replaced with the code generated by the hooking process. It redirects execution of the code to the hooking process. The hooking process has generated code at that address.

- Performs the action that hooks the API call
 - Recording the API call
 - Modifying the API call
 - Blocking the API to stop execution
- Performs the replaced instruction
- Jumps execution back to the original function

As the original function then continues execution as usual, neither the code calling the API nor the system kernel are aware that the function call has been intercepted.

Malware Unhooking API Hooks

Email Header

- From: Alhaji Nasiru <sales@gossipnewspro.info >
- To: <-Redacted>-.com>
- Subject: New Purchase Order for August
- Date: Sun, 28 Jul 2019 16:41:52 -0700
- Attachment: Signed-revised-PI.xls

Downloader

- Filename: Signed-revised-PI.xls
- Size: 82 KB (83968 bytes)
- MD5: C081E4AA1FBEC4857E88E4F91FE90E
- SHA-1: 1F6527CBD8BC83132A89C4F66A897A576259C4A1
- SHA-256: 42BD54E60C86AE02BCD9BCD02FA82C9D77D831F3EED77DD924E2E6976B9A5808



Security Boulevard asks for your consent to use your personal data to:

- Personalised advertising and content, advertising and content measurement, audience research and services development
- Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.



THREATLOCKER®

Do you know what is running in your environment?

[Check Now!](#)

Most Read on the Boulevard

- Book ‘Infinite Money Glitch’ — Idiots Lured by JPMorgan
- Spooky Spam, Scary Scams: Halloween Threats Rise
- NTT Data Taps Palo Alto Networks for MXDR Service
- Proofpoint Boosting Data Security with Normalyze Acquisition
- UnitedHealth Hires Longtime Cybersecurity Executive as CISO
- More Than Just a Corporate Wiki? How Threat Actors are Exploiting Confluence

Industry Spotlight »

Ô! China Hacks Canada too, Says CCCS

Dropper

- Filename: v4bc6f.exe [Win32.Trojan.Injector]
- File size: 936 KB (958464 bytes)
- MD5: 97BD950CA1FBD49A632A876A05E7ACEF
- SHA-1: 6FD6E4B676BD363B817F54F067684A14BA31E053
- SHA-256: 851AC0EF0956156EFCDDDB15288A6DF82009940D58F851D006732675F3B9AD1D

Modern malware typically relies on polymorphism and obfuscation techniques to evade static detection by signature-based detection technologies such as anti-virus. EDR tools work differently by monitoring system activity and flagging suspicious events if there is a deviation from normal application behaviour or if there is a match against known malicious patterns. Most of these events are generated by hooking APIs. Some security solutions also use API hooks to block malicious processes if a suspicious event is triggered.

When analysing this malicious sample we noticed some unique code that was modifying the memory-mapped ntdll.dll before launching its payload, Agent Tesla (bin.exe). The malware allocates the shellcode and then performs the following actions:

- Call NtProtectVirtualMemory in ntdll.dll’s address space to change its memory permissions of the region to PAGE_EXECUTE_READWRITE
- Removes the API hooks from memory
- Call NtProtectVirtualMemory to change the memory permissions of the region to PAGE_EXECUTE_READ
- After removing the hooks, it e

Figure 4: Removing API hooks from memory


The malicious code loads the address of the ntdll.dll into the register `eax` and then scans through the memory of the loaded module. The instruction at `0x004A0A50` is incrementing the value of `eax` by 1. The instruction at `0x004A0A51` is comparing the value of `eax` with `0x004A0A50`.

The first check at `0x004A0A51` is for the value of `Wow64Transition`. If it’s found, the instructions starting at `0x004A0A5B` are performed. In sequence these are:


The result of writing out the 5 bytes (4 for `eax` and one for `0xB8`) is to replace any hooking instruction (such as `jmp 0x004F0012` in the previous example) with the original instruction that was there (which is `mov eax, 50` in the previous example).

The end result is that the malicious code can now call system APIs, safe in the knowledge that its requests won’t be monitored or blocked by any hooks.

This unhooking isn’t an issue for Bromium Secure Platform as the malicious activity will still all be contained inside a micro-virtual machine (uVM) where hardware-backed isolation is used for protection.

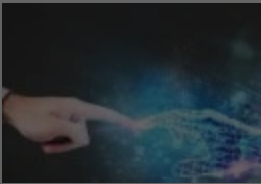


UnitedHealth
Hires Longtime
Cybersecurity
Executive as CISO




Small Businesses
Boosting
Cybersecurity as
Threats Grow:
ITRC

Top Stories »



GreyNoise: AI’s
Central Role in
Detecting
Security Flaws in
IoT Devices



Microsoft’s
Controversial
Recall Feature
Release Delayed
Again



CISA Strategic
Plan Targets
Global
Cooperation on
Cybersecurity

Security Humor »



IT’S RIDICULOUS THAT WELLS WORK.

Randall Munroe’s XKCD ‘Wells’

Download Free eBook

Agent Tesla Payload

- Filename: bin.exe [ByteCode-MSIL.Spyware.lelib]
- File size: 331.5 KB (339456 bytes)
- MD5: 640CA1048F2AED048CB209234FA080B9
- SHA-1: 58790A758B31E80648DB288BA86F49F7DC05D89B
- SHA-256: 53997AF9CF992BF7A97E54F79A1474A1C0023133D7B97B861A278BAA238C9421

The post [Agent Tesla: Evading EDR by Removing API Hooks](#) appeared first on [Bromium](#).

Recent Articles By Author

- [Ransomware Goes Fileless, Uses Malicious Documents and PowerShell to Encrypt Files](#)
- [Reawakening of Emotet: An Analysis of its JavaScript Downloader](#)
- [Dridex’s Bag of Tricks: An Analysis of its Masquerading and Code Injection Techniques](#)



More from Ratnesh Pandey



Agent Tesla, api, EDR, hooking, ntdll...

← [Movie Tickets Service Exposed](#)

The



Security Boulevard

Security Boulevard asks for your consent to use your personal data to:



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.



Join the Community

Add your blog to Security Creators Network

Write for Security Boulevard

Bloggers Meetup and Awards

Ask a Question

Email:
info@securityboulevard.com

Useful Links

About

Media Kit

Sponsor Info

Copyright

TOS

DMCA Compliance Statement

Privacy Policy

Related Sites

Techstrong Group

Cloud Native Now

DevOps.com

Digital CxO

Techstrong Research

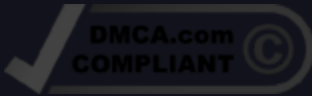
Techstrong TV

Techstrong.tv Podcast

DevOps Chat



DevOps Dozen

DevOps TV





Security Boulevard asks for your consent to use your personal data to:

-  Personalised advertising and content, advertising and content measurement, audience research and services development
-  Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.

