ultraviolet

CONFIDENTIAL

THREAT REPORT:

How Threat Actors Are Using ScareCrow to Bypass EDR Tools

Services Performed By:
UltraViolet Cyber
Jacob Wyatt
(443) 351-7630
info@uvcyber.com

Published Date:
10/30/2023

Doc ID: ECORP_SUM_07032023_v1.1

Contents

1 Executive Summary

As technology progresses, defensive as well as offensive measures for security constantly evolve. Security researchers consistently find new ways to exploit widely used software and systems that allow malicious actors to go undetected before the “good” guys catch on. It’s because of this cat-and-mouse game that tools like ScareCrow need to be studied, providing blue teams with the knowledge to better understand the methods that malicious actors use to evade detection. In this article, we will discuss the use cases for the tool, ScareCrow, a payload creation framework designed for red team cybersecurity purposes.

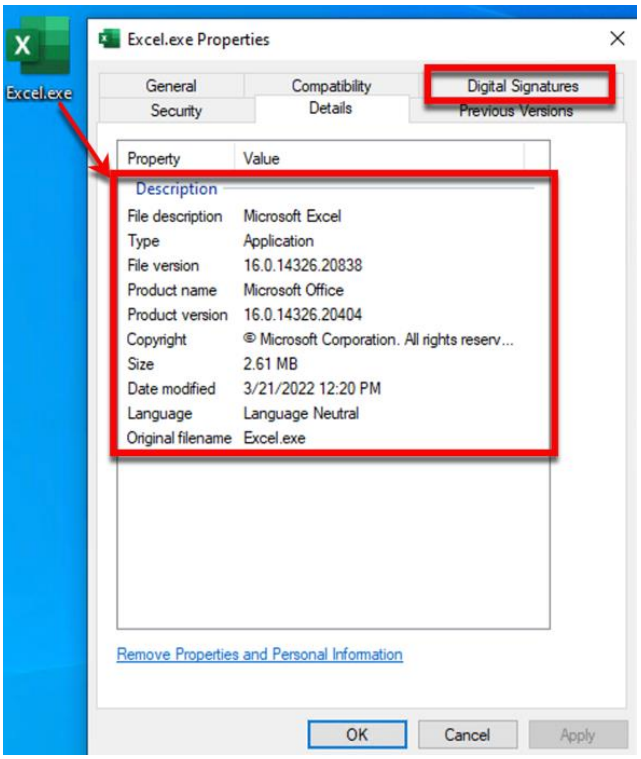
2 Technical Analysis

ScareCrow, as seen in the public GitHub repository located at https://github.com/optiv/ScareCrow, is a free and sophisticated payload creation framework used in cybersecurity for generating loaders that facilitate side loading into legitimate Windows processes, effectively bypassing Application Whitelisting controls. In this context, A "loader" is a piece of software designed to load and execute malicious code, such as a virus or a backdoor, into a computer system. It's essentially a helper that gets the main malicious software running on the target machine, often by injecting it into a legitimate process to avoid detection by security software. ScareCrow’s primary function is to evade Endpoint Detection and Response (EDR) systems by removing their hooks from the system's Dynamic Link Libraries (DLLs) in memory. Hackers may utilize ScareCrow for its ability to manipulate memory permissions, use indirect syscalls for stealth, and leverage code signing certificates, making it a very viable tool for bypassing security mechanisms, deploying malware without detection, and maintaining persistence within a compromised system. Simply put, ScareCrow is a tool used by malicious actors to plant malicious software into a computer without being caught by security systems. It tricks the computer into thinking the “bad” software is “good”, allowing hackers to maintain remote access on the system and exfiltrate data. The process may sound complicated; however, it is quite easy to understand when broken down:

Most modern EDR systems use user-mode API hooking to monitor activities by the system and user. The EDR intercepts function calls to NTDLL.DLL, a key Windows DLL containing essential API functions, by injecting their own DLL into the process space and hooking functions to track and potentially stop suspicious actions like process creation, file opening, or code injection. Previously, a hacker could block non-Microsoft DLLs from loading to prevent this, but many EDRs now use Microsoft-signed DLLs, which circumvent this defense. ScareCrow can be used to counter this by encrypting shellcode from tools like Cobalt Strike or Metasploit with AES encryption, avoiding static detection. Upon execution, it loads a clean

version of NTDLL.DLL (and others like kernel32.dll, kernelbase.dll) from disk, replacing the hooked versions and removing EDR surveillance. It then uses syscalls to load, decrypt, and execute the shellcode in memory, evading both hooks and other system monitoring techniques like Event Tracing for Windows.

Additionally, ScareCrow can spoof code signing certificates and modify file attributes to disguise its payloads as legitimate files. Ultimately, this allows a malicious actor to maintain an undetected presence on a system, disguising itself as a benign executable or process. Here is the result after disguising a Cobolt Strike beacon as excel using ScareCrow:



(Photo from the official ScareCrow Github Repo: https://github.com/optiv/ScareCrow)

As we can see with the screenshot, the “Excel.exe” is actually a Cobolt Strike beacon disguised as a regular, signed copy of Microsoft Excel. With the malware disguised as legitimate software, it makes detecting the product very difficult; however, there are methods in place in which we utilize to make detection of such malware easier.

3 What UltraViolet Cyber is Doing

- We are continuing to monitor for unusual process behavior in the logs, such as a process trying to access or modify system DLLs, which could indicate an attempt to replace them with clean versions such as ScareCrow does.
- We are also monitoring for unexpected or anomalous network traffic patterns that could indicate command and control (C2) communication or data exfiltration attempts.
- Analyze logs for unusual system call patterns, especially those related to memory manipulation, which ScareCrow might use to unhook EDR systems.

(443) 351-7630 | info@uvcyber.com

4 What Customers Can Do

- Conduct regular cybersecurity training sessions to educate employees about the latest threats, phishing tactics, and safe computing practices.
- Keep all operating systems, software, and firmware up to date with the latest security patches to close off vulnerabilities that could be exploited.
- Segment the network to limit lateral movement and contain potential breaches within isolated segments.
- Regularly back up critical data and ensure that backups are stored securely and can be restored quickly in case of an incident.

5 References

- "EDR Evasion Part I: Understanding Scarecrow." *Ptr0x1.com*, 7 Nov. 2022, ptr0x1.com/posts/edr-evasion-part-i-understanding-scarecrow/. Accessed 31 Oct. 2023.
- Svoboda, Adam. "Evading EDR in 15 Minutes with ScareCrow." *Adam Svoboda*, 30 July 2021, adamsvoboda.net/evading-edr-with-scarecrow/. Accessed 31 Oct. 2023.
- Tylous. "ScareCrow." *GitHub*, 31 Oct. 2023, github.com/optiv/ScareCrow. Accessed 31 Oct. 2023.

(443) 351-7630 | info@uvcyber.com