AVALON Cyber

# **Case Study:** Incident Response – Cybercriminal attempts to execute a ransomware attack on Christmas Day

Several instances of this program were attempting to execute–and each one was blocked by our sensor

## The Incident

On December 25, 2019, Avalon Cyber received multiple Managed Detection & Response (MDR) alerts around 1:00 a.m. about potentially malicious attack attempts occurring on a client's internal network system.

## The Plan

To conduct incident response (IR) analysis to determine legitimacy of the attack attempt. Once confirmed, we were to contact the client to provide details of the cyber incident and provide direction and support for remediation procedures.

## The Investigation

Through our IR analysis, our team discovered three separate attack attempts on a Citrix server early in the morning on December 25, 2019. The first attempt showed the adversary logging into the Citrix server and running several executable files to determine exploitable vulnerabilities on the system.

We determined that one program, named *EladErex.exe*, was used to find vulnerabilities related to WannaCry, NotPetya, and any other EternalBlue based attacks. Another program used to gain insight into the system was *PCHunter64.exe*, a very powerful security utility that allows users to acquire knowledge about the inner workings of Windows. Several instances of this program were attempting to execute–and each one was blocked by our sensor. The last program the bad actor used, named *gmer.exe*, allowed for the detection and removal of rootkits (software programs that allow unauthorized users to seize control of a computer system without being discovered), which they performed to cover their tracks and prevent us from discovering their activities.

The second and third attempted attacks utilized the same strategy as the first to determine exploitable vulnerabilities. With each execution blocked, the adversary then changed tactics and attempted to launch an application named *mimikatz.exe*, a tool commonly used by attackers to steal credentials and escalate privileges. Again, the Avalon Cyber sensor was able to block this program from executing. One more attempt was made by the adversary to launch Mimikatz from a command window, but once this attack was also blocked, criminal activity ceased.

## The Result

The Avalon Cyber team was able to successfully contain the host from further attack strategies and notify our client of the incident. The client has since had their internal incident team bring down the server to begin a full rebuild.

AVALON Cyber

## QUESTIONS?

For more information on Incident Response or any of our services, please contact:

**Ian Gattie**
Director of Marketing
716.995.7777
ian.gattie@teamavalon.com