Bennett Hall

Professor Anthony Candeias

CISC 6680, Intrusion Detection

May 5th, 2021

Lab 6: Endpoint Security

1. Executive Summary

My name is Bennett Hall and I am a security investigator working on behalf of Global Comm. Global Comm has asked me to generate an incident report about malicious activity that has been detected on their computer WINDEV1911EVAL. I used Crowdstrike Falcon to investigate the incident. On April 30th, 2021 Crowdstrike Falcon alerted us to an attack that stemmed from a malicious executable file, or exe, on device WINDEV1911EVAL. The attacker was able to use their malicious executable file to gain entry, escalate their privileges, establish persistent access to keep coming back, executed a powershell to steal information and then used a program called MimiKatz that is commonly used to steal passwords on Windows machines.

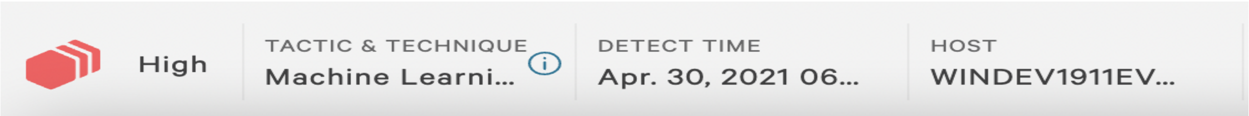
Currently Global Com enjoys a stellar reputation and the company has the trust of its customers, employees, and the public alike. A successful malicious executable file attack harms Global Com's reputation and wrecks the trust that the company has worked so hard to develop. The successful malicious executable gave the attacker access to Global Com's network, allowed the attacker to steal credentials, and inject malware on the target machine. The success of this attack will cause current customers to question whether or not they should continue to do business with a company that may not be taking sufficient precautions to prevent cyberattacks. Prospective customers are much less likely to work with Global Com if the company cannot offer a level of confidence in their systems. All of this will, potentially, lead to a reduction in the bottom line of Global Com.

Global Com can take actions to remediate the incident. Global Com needs to get WINDEV1911EVAL off of the network and do a static analysis of the malicious code. Once The analysis is complete Global Com needs to use anti-malware software to remove the malware. Finally Global Com needs to restore the target machine to a previous state.

2. Technical Overview

The malicious executables were accessed from port 4444. In this incident Crowdstrike Falcon issued 11 detection alerts. There was a lot of activity during the time of the attack, but for the sake of brevity I will focus on the 11 detections. The first alert was generated by Crowdstrike Falcon at 6:07 local time. The first alert was detected by sensor-based machine learning (ML) that analyzes executables as they run. Figure 1 shows this alert.

Figure 1



High

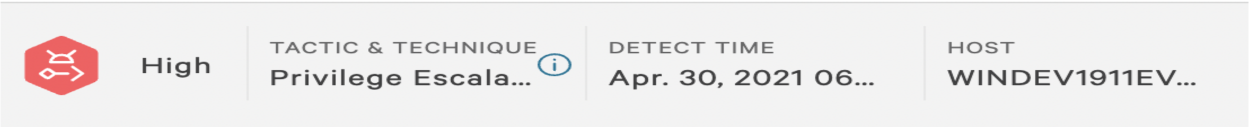
TACTIC & TECHNIQUE
Machine Learni...

DETECT TIME
Apr. 30, 2021 06...

HOST
WINDEV1911EV...

Crowdstrike Falcon alerted us to the malware, from malicious executable files, six times between 6:07 and 6:23 on computer WINDEV1911EVAL. This gave an attacker entry into the target machine. At 6:26 Crowdstrike Falcon alerted that the attacker attempted to escalate their privileges by bypassing account controls. This allowed the attacker to perform admin level privileges. Figure 2 shows this action.

Figure 2



High

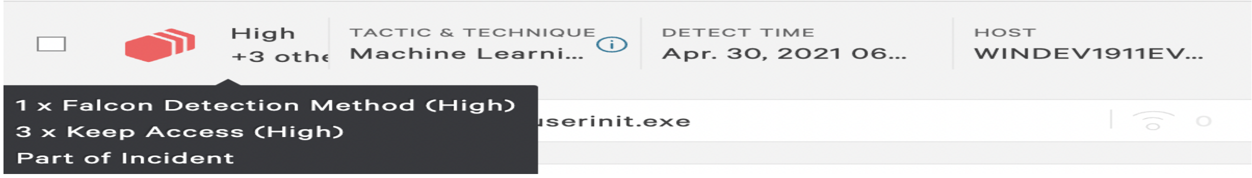
TACTIC & TECHNIQUE
Privilege Escala...

DETECT TIME
Apr. 30, 2021 06...

HOST
WINDEV1911EV...

At 6:27 the attacker sought to create a method of persistence that allowed them to continue access to WINDEV1911EVAL as well as cover their tracks to avoid detection. The attacker was able to evade Global Com defenses by injecting malicious code, a process injection, using meterpreter payload into the Windows DLL library on WINDEV1911EVAL. Figure 3 shows this action.

Figure 3



High
+3 othe

TACTIC & TECHNIQUE
Machine Learni...

DETECT TIME
Apr. 30, 2021 06...

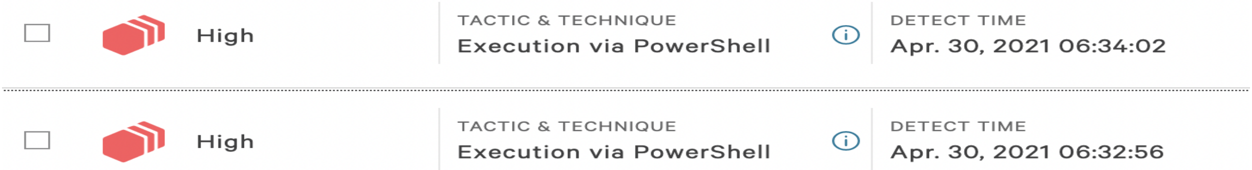
HOST
WINDEV1911EV...

1 x Falcon Detection Method (High)
3 x Keep Access (High)
Part of Incident

serinit.exe

At 6:32 and again at 6:34 the attacker executed a powershell exploit kit that gave them the ability to steal data. Figure 4 shows this action.

Figure 4



High

TACTIC & TECHNIQUE
Execution via PowerShell

DETECT TIME
Apr. 30, 2021 06:34:02

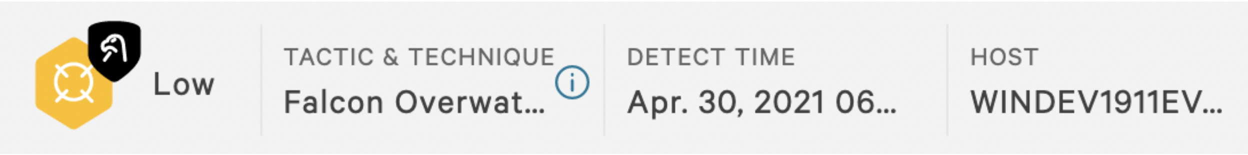
High

TACTIC & TECHNIQUE
Execution via PowerShell

DETECT TIME
Apr. 30, 2021 06:32:56

Powershell does require admin privileges to run so we can assume that the earlier attempt to escalate privileges was successful. Finally, at 6:42, MimiKatz was run against our target machine, WINDEV1911EVAL. Mimikatz is used to steal passwords on Windows systems. Figure 5 shows this action.

Figure 5



Low

TACTIC & TECHNIQUE
Falcon Overwat...

DETECT TIME
Apr. 30, 2021 06...

HOST
WINDEV1911EV...

Crowdstrike Falcon used multiple detection techniques to alert us on the malicious activity. One of those techniques was machine learning via sensor-based machine learning. The sensor-based machines learning technique analyzes unknown executables as they run on a system and compares them with known malware. Sensor-based ML can run when a host is offline. The sensor-based machine learning altered us to the malicious executable file execution occurring on WINDEV1911EVAL. Another technique used was the Falcon Overwatch. Falcon Overwatch flagged suspicious activity. The Falcon Overwatch notification was flagged as low priority, but it's still recommended that this incident be investigated for suspicious activity. This could be a false positive or it could be an actual threat. In this case it altered on the execution of MimiKatz. We know that the attacker got into the target computer and was trying to steal access credentials so it must be investigated further given what we know about the attack.

Malicious executables are typically executed by a user and allow an attacker to gain access into a system. In this attack, the malicious executable file injected code into the target machine. Once inside of a system the attacker attempted to infect the target computer with malware to escalate their privileges, and steal login credentials. Often attackers will also create a method of persistence or backdoor that allows them to continue coming back to a target over and over, which the attacker did in this attack. The attacker used a few different malicious executables including powershell, CMP, and a payload exe.

3. Remediation Plan

We have examined the attack and its technical capabilities. We have also discussed how to remove the malicious executable from WINDEV1911EVAL. How can Global Com prevent this from happening again? Here are a few recommendations:

1) Create a whitelist of approved files types. This reduces the attack surface by eliminating common malicious file types, making it much harder for attackers to use malicious executables in the future.
2) Verify files before they are uploaded. Even with a whitelist of approved files it's still possible for attackers to execute malicious files. Verifying files before upload prevents attackers from sneaking around the whitelist.
3) Set maximum file sizes and names. This further reduces the attack surface and decreases the attackers chance of successfully executing malicious files on a target system.
4) Conduct regular scans for malware. This should be done frequently so that attackers, if successful, are only in the system for a limited time before being caught.
5) Review existing files for malware and remove all dated and unnecessary files that may contain malware. This proactively removes malicious executables before they are executed.
6) Segment the network. If an attacker does get into a target system they will have limited access within a network.
7) Encrypt all data, including access credentials. If an attacker does get access to a system and steals data it will still be worthless if the data is encrypted.
8) Keep all systems updated and patched. Reduces attackers ability to take advantage of outdated systems.
9) Conduct user training on malicious executables. This teaches employees how to be safe and also what to do if they suspect that they have become a victim of an attack.

10) Have firewalls on the network and all hosts, antivirus software on all devices, email gateways, and any useful anti-malware software. These systems block and remediate malicious executables.