Detecting CONTI with ML

Based on real events

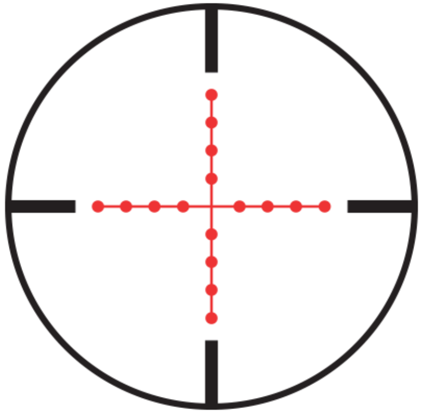
The Ransomware Attack

Global Company

The attack could spread

CONTI

TOP Threat Actor from Russia using Cobalt Strike



Worldwide Scope

5k Servers + 350 DCs + 12k Laptops

The Breach. Day 0

SOC Alert!

Pre-Ransomware tools found

5 infected hosts

5 days since intrusion

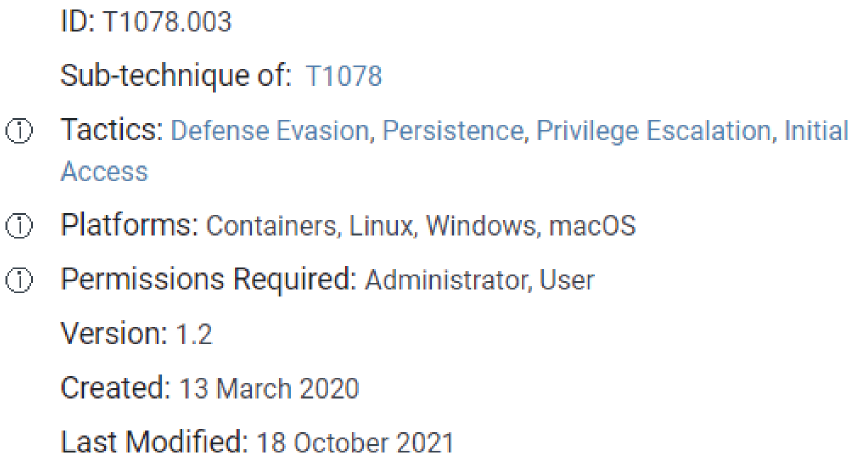
Possibly spread

Detecting The Enemy

We will detect the intrusion in different phases

NEW

TA0001: Initial Access
T1078.003: Malicious Logons



ID: T1078.003

Sub-technique of: T1078

ⓘ Tactics: Defense Evasion, Persistence, Privilege Escalation, Initial Access

ⓘ Platforms: Containers, Linux, Windows, macOS

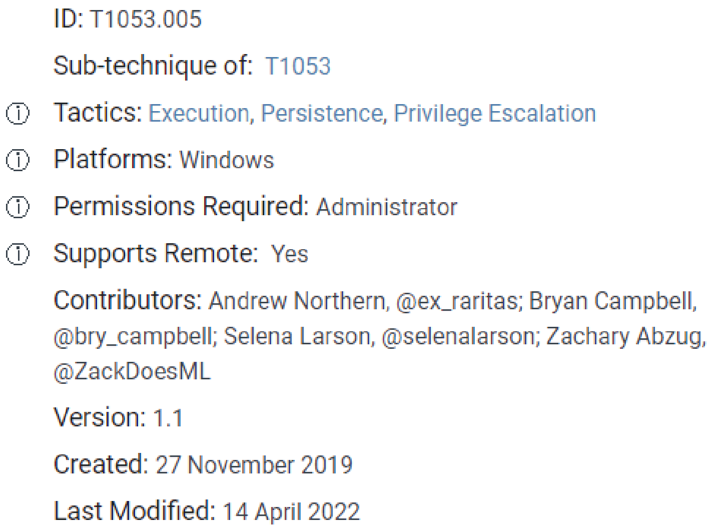
ⓘ Permissions Required: Administrator, User

Version: 1.2

Created: 13 March 2020

Last Modified: 18 October 2021

TA0003: Persistence
T1053.005: Scheduled Tasks



ID: T1053.005

Sub-technique of: T1053

ⓘ Tactics: Execution, Persistence, Privilege Escalation

ⓘ Platforms: Windows

ⓘ Permissions Required: Administrator

ⓘ Supports Remote: Yes

Contributors: Andrew Northern, @ex_raritas; Bryan Campbell, @bry_campbell; Selena Larson, @selenalarson; Zachary Abzug, @ZackDoesML

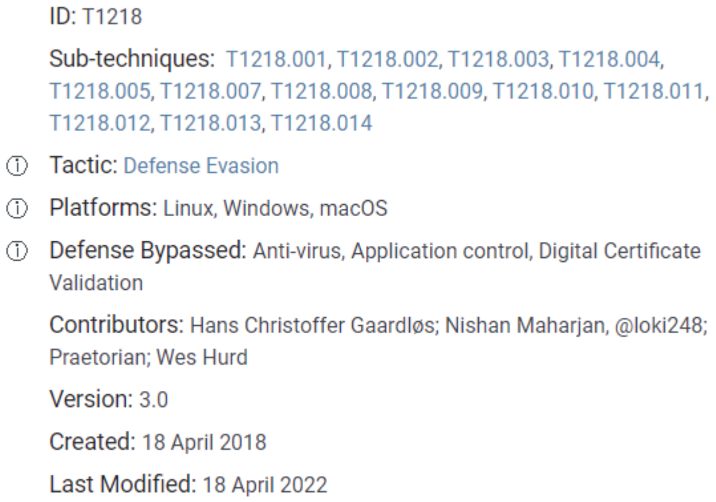
Version: 1.1

Created: 27 November 2019

Last Modified: 14 April 2022

Detecting Cobalt Strike with prefetch

TA0005: Defense Evasion
T1218: System Binary Proxy Execution



ID: T1218

Sub-techniques: T1218.001, T1218.002, T1218.003, T1218.004, T1218.005, T1218.007, T1218.008, T1218.009, T1218.010, T1218.011, T1218.012, T1218.013, T1218.014

ⓘ Tactic: Defense Evasion

ⓘ Platforms: Linux, Windows, macOS

ⓘ Defense Bypassed: Anti-virus, Application control, Digital Certificate Validation

Contributors: Hans Christoffer Gaardløs; Nishan Maharjan, @loki248; Praetorian; Wes Hurd

Version: 3.0

Created: 18 April 2018

Last Modified: 18 April 2022

New Lethal Forensicator Technique!