



# **Assessing the importance of modern security tools and frameworks to help detect and defend against Cozy bear**

## **Internship final draft**

Niall O'Brien

x20196474@student.ncirl.ie

Msc in Cyber Security

National College of Ireland

# Abstract

Modern security tools and frameworks provide an important layer of security for computer systems and networks. Threat hunting and defensive tools are setup to help detect and prevent attacks, to alert those tasked with defending systems of possible intrusions on their network. Nation state Cyber threat actors continue to evolve in targeting individuals, organizations, and governments worldwide in 2022. The knock-on effect of this is a huge market for security vendors to push their products to entice organisations to try and stay one step ahead of the bad guys. Choosing the right tools is the challenge all organisations face today.

In this study, this author assessed an array of modern security tools and frameworks to help give network defenders a clearer path on how to defend against a malicious hacking group known as Cozy bear, aka APT29. A nation state backed Cyber group, to understand it's key identifiers in relation to attacks that have been seen in the wild in recent years. The innovative aim of this research is to show that through the collective use of threat hunting tools such as Velociraptor and Hayabusa, a defensive tool called Snort in alignment with the security frameworks Mitre Attack and Cyber Kill chain, that it is possible to defend against Cozy bear. The final piece is related to clause 9.1 of the ISO27001 framework, monitoring and measuring, to show how we can satisfy this clause with the use of the tools used in this paper.

Results produced in this paper will aim to show Cozy bear can be kept at bay through a combination of security tools and frameworks.

Further research needs to be carried out into the use of the tools and frameworks outlined in this paper. A one shoe fits all, security tool combined with a framework that prevents or detects an attack such as Cozy bear would make network defenders jobs easier.

**Keywords:** Nation State, Cozy bear, APT29, Velociraptor, Hayabusa, Mitre Attack, Cyber Kill Chain, ISO27001

## Contents

I.	INTRODUCTION .....	4
II.	Literature Review .....	5
	A. <b>Overview</b> .....	5
	B. <b>Cozy Bear</b> .....	5
	C. <b>Velociraptor</b> .....	5
	D. <b>Hayabusa</b> .....	6
	E. <b>Snort</b> .....	7
	F. <b>Mitre Attack</b> .....	7
	G. <b>The Cyber Kill Chain</b> .....	7
	H. <b>ISO27001 monitoring and measuring</b> .....	8
III.	research methodology .....	9
	A. <b>Approach</b> .....	9
	B. <b>Velociraptor</b> .....	9
	1) <b>Artifacts</b> .....	11
	2) <b>Main Results</b> .....	17
	C. <b>PEStudio</b> .....	18
	1) <b>Yara</b> .....	19
	D. <b>Hayabusa Tool</b> .....	19
	1) <b>Main Results</b> .....	20
	E. <b>Neo4j</b> .....	21
	F. <b>Snort Tool</b> .....	23
IV.	Design Specification .....	26
	A. <b>Mitre Attack</b> .....	26
V.	Implementation .....	28
	A. <b>Cyber Kill chain</b> .....	28
	B. <b>ISO27001 – Monitoring and Measurement</b> .....	31
VI.	Conclusions .....	32
VII.	References .....	33

## I. INTRODUCTION

Nation state actors work on behalf of governments to target organizations, individuals, or governments worldwide, they basically have a 'license to hack!'. None more so than a Russian hacking group known as Cozy bear, aka APT29, Fritillary, the Dukes, Nobelium, Dark Halo and many more assumed names given by various cybersecurity firms. This group has been known to work directly on behalf of one or more Russian intelligence agencies, in effect working in conjunction with the very top echelons of the Russian government. Targets have included governments departments, including energy, military, diplomatic and telecom sectors in the US, Germany, South Korea and Uzbekistan.

The research problem the author attempts to solve is which modern security tools and frameworks organisations big or small should adopt to help protect company assets.

The importance of this study aims to give network defenders a clear path into the use of modern security tools and frameworks to help in the defence of the Cozy bear threat group in their attempts to infiltrate networks worldwide.

An output of this research paper will be to show how it is possible to defend against Cozy bear and similar nation state hacking groups with the use of threat hunting, defensive tools and frameworks.

The authors motivation to research this topic is rooted in the day-to-day struggle organisations face in the fight to stay one step ahead of the bad guys and protect company assets.

## II. LITERATURE REVIEW

### A. Overview

The literature review section of this paper will take a look at the Russian hacker group Cozy bear, referencing leading security vendors to take a deep dive to try understand its origins, signature attack profiles and organisations it has targeted. The rest of the review will take a look at security tools and frameworks to help defend against it.

### B. Cozy Bear

The Cyber threat landscape has continued to evolve over the years with any user connected to the internet fair game to the nefarious threat actors that lurk out there. None more so than a Russian Cyber espionage group known as Cozy bear<sup>1</sup> and according to one of the industry leaders in Cybersecurity in protecting endpoints CrowdStrike is an adversary of Russian-origin, more likely to be acting on behalf of the Foreign Intelligence Service of the Russian Federation. A nation state controlled and backed hacker group that has been known to use large-volume spear phishing campaigns to help deliver several malware types to organizations across the world, in an attempt to gain access to networks with the aim of collecting information required by Russian operational directorates<sup>2</sup>.

According to another leading security vendor Broadcom<sup>3</sup> Advanced Persistent Threat (APT) groups such as Cozy bear (aka APT29, Firtillary, the Dukes) are widely classified as organizations that “initially confined itself to spying campaigns, focusing on governments, the military, and think tanks in the U.S. and Europe. It later became involved in more subversive operations and was implicated (along with APT28) in disruptive attacks prior to the 2016 U.S. presidential election.” Another leading security vendor SOCRadar<sup>4</sup> claim that APT29 aka Cozy bear were behind the SolarWinds supply chain attack in 2019-2020 and targeted Denmark’s central bank (Denmark’s National Bank) and installed malware that enabled them to access their network and remain undetected for over 6 months.

One such malware seen and used in the wild to target COVID-19 vaccines according to the UK National Cyber Security Centre is known as Wellmess<sup>5</sup> a “lightweight piece of malware that enables its operators to execute shell commands, as well as to upload and download files on the compromised system”. Later in this paper the author will look at an example of the Wellmess malware downloaded from the web to explain how it can be detected.

### C. Velociraptor

Threat hunting tools have evolved over the years and none more so than a relatively new tool called Velociraptor<sup>6</sup> developed by Michael Cohen. It is known as both a triaging tool and an endpoint monitoring and collection tool that implements a powerful Velociraptor Query Language (VQL) engine.

---

<sup>1</sup> “Adversary: Cozy Bear - Threat Actor,” CrowdStrike Adversary Universe, no. 1, accessed August 14, 2022, <https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/>.

<sup>2</sup> “Main Directorates of the Armed Forces General Staff,” no. 2, accessed August 14, 2022, <https://www.globalsecurity.org/military/world/russia/mo-general-staff-1.htm>.

<sup>3</sup> Threat Hunter Team, “Attacks Against the Government Sector (White Paper),” n.d., no. 3.

<sup>4</sup> “APT Profile: Cozy Bear / APT29,” SOCRadar® Cyber Intelligence Inc., November 16, 2021, no. 4, <https://socradar.io/apt-profile-cozy-bear-apt29/>.

<sup>5</sup> “Advisory: APT29 Targets COVID-19 Vaccine Development,” no. 5, accessed August 14, 2022, <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development>.

<sup>6</sup> “Welcome :: Velociraptor - Digging Deeper!,” no. 6, accessed August 14, 2022, <https://docs.velociraptor.app/>.

Velociraptor was created and heavily influenced by 3 existing forensic tools designed by both Google and Facebook. Googles GRR Rapid Response Framework<sup>7</sup> a powerful open-source tool for enterprise forensic investigations. Googles Rekal framework<sup>8</sup> an “open collection of tools, implemented in Python under the Apache and GNU General Public License, for the extraction and analysis of digital artifacts computer systems.” This tool is no longer in circulation and was discontinued in 2011.

Facebooks OSQuery framework<sup>9</sup> is a powerful security tool to allow the user write SQL based queries easily and effectively to explore operating systems. It is an operating system instrumentation, monitoring, and analytics framework powered by SQL. With OSQuery, SQL tables represent the current state of operating system attributes for example running processes.

Velociraptor allows packaging VQL queries inside programs called Artifacts<sup>10</sup> An artifact is a structured readable YAML file, containing a query with a name attached to it. It allows users to search for the query by name to run on an endpoint to collect information to help locate malicious files.

#### **D. Hayabusa**

As part of this authors research, it was important to look at other modern software tools that can assist network defenders in the fight against Cozy bear threat group. Hayabusa<sup>11</sup> is a Windows event log fast forensics timeline generator and threat hunting tool created by the Yamato Security group in Japan. Written in a programming language called Rust<sup>12</sup>, it is a very fast and memory-efficient language with no runtime or garbage collector, so ideal for threat hunting scenarios. Known to be very reliable in relation to memory and thread safety, which enables the elimination of many classes of bugs at compile-time. Hayabusa as we will see later in this paper can be run on a single windows machine for example for live analysis. It also can be used to gather logs from multiple systems for offline analysis or from within the Velociraptor tool using the Hayabusa artifact for enterprise threat hunting and incident response. A paper from Abe et al<sup>13</sup> in 2017 on the Hayabusa tools performance, they claim that the tool required only 8 seconds to convert 1.2 million log messages into a database file and 5 seconds to search a keyword from 1.7 billion records. They also state in a standalone environment in comparison to a distributed environment, the stand-alone version of Hayabusa was approximately 27 times faster.

---

<sup>7</sup> “What Is GRR? — GRR Documentation,” no. 7, accessed August 14, 2022, <https://grr-doc.readthedocs.io/en/v3.2.1/what-is-grr.html>.

<sup>8</sup> “Rekal Discontinuation,” Python (2014; repr., Google, August 3, 2022), no. 8, <https://github.com/google/rekal>.

<sup>9</sup> Import User, “Introducing Osquery,” *Engineering at Meta* (blog), October 29, 2014, no. 9, <https://engineering.fb.com/2014/10/29/security/introducing-osquery/>.

<sup>10</sup> “Artifacts :: Velociraptor - Digging Deeper!,” no. 10, accessed August 14, 2022, <https://docs.velociraptor.app/docs/gui/artifacts/>.

<sup>11</sup> do son, “Hayabusa v1.4.3 Releases: Windows Event Log Fast Forensics Timeline Generator and Threat Hunting Tool,” *Penetration Testing*, December 31, 2021, no. 11, <https://securityonline.info/hayabusa-windows-event-log-fast-forensics-timeline-generator/>.

<sup>12</sup> “Rust Programming Language,” no. 12, accessed August 14, 2022, <https://www.rust-lang.org/>.

<sup>13</sup> Hiroshi Abe et al., “Hayabusa: Simple and Fast Full-Text Search Engine for Massive System Log Data,” in *Proceedings of the 12th International Conference on Future Internet Technologies*, CFI’17 (New York, NY, USA: Association for Computing Machinery, 2017), no. 13, <https://doi.org/10.1145/3095786.3095788>.

## **E. Snort**

Threat hunting tools such as Velociraptor and Hayabusa are extremely useful to network defenders in discovering if their systems have been infiltrated by a bad actor. But intrusion prevention systems such as Snort<sup>14</sup> can also help assist in preventing threat actors from infiltrating a network in the first place. It's a powerful open source IPS (intrusion prevention system) tool that is made up of multiple rules to help locate malicious network activity to match packets against these rules to generate alerts. While it is relatively straight forward to understand and configure your own rules as proposed by Rapid 7<sup>15</sup> users can also get access to Community rules which are basically all the rules that have been submitted by members of the open-source community or Snort integrators, which is updated and released weekly.

## **F. Mitre Attack**

While it is essential to have software tools to assist those tasked with defending against Cozy bear to prevent Cyber breaches from happening, it's also critical that they follow and abide by a Cyber security framework such as the Mitre Attack. As stated by one of the world's leading Cyber Security companies Palo Alto Networks the Mitre Attack framework<sup>16</sup> "is a comprehensive matrix of tactics and techniques designed for threat hunters, defenders, and red teams to help classify attacks, identify attack attribution and objective, and assess an organization's risk. Organizations can use the framework to identify security gaps and prioritize mitigations based on risk."

While the article from Palo Alto describes in detail the makeup of the Mitre Attack a paper by Xiong et al<sup>17</sup> in 2021 propose a new threat modelling language for enterprise systems with the mitre attack acting as a knowledge base. They state the mitre attack provides useful information for a threat modelling language due to its focus on "assets such as (e.g., Computer, Service, OS, Firewall, Internal and External Network), attack steps (e.g., Spearphishing Attachment, User Execution, and Data Destruction), and defences (e.g., Privileged Account Management, Execution Prevention, and Network Segmentation). Based on a system model and using available tools, enterpriseLang allows 1) analysing weaknesses related to known attack techniques and 2) providing mitigation suggestions for these attacks. Therefore, stakeholders of an enterprise can assess threats to their enterprise IT environment and analyse what security settings that could be implemented to secure the system more effectively."

## **G. The Cyber Kill Chain**

The Cyber Kill Chain<sup>18</sup> is one of the most important security frameworks developed in 2011 by a world leading security and aerospace company Lockheed Martin. The Cyber Kill chain process "sets out the stages of a possible cyberattack and allows organizations to identify and protect themselves against threats, such as data theft, malware, ransomware, or network breaches. The term originates from the

---

<sup>14</sup> "Snort - Network Intrusion Detection & Prevention System," no. 14, accessed August 14, 2022, <https://www.snort.org/>.

<sup>15</sup> "Understanding and Configuring Snort Rules | Rapid7 Blog," Rapid7, December 9, 2016, no. 15, <https://www.rapid7.com/blog/post/2016/12/09/understanding-and-configuring-snort-rules/>.

<sup>16</sup> "What Is the MITRE ATT&CK Framework? - Palo Alto Networks," no. 16, accessed August 14, 2022, <https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-framework>.

<sup>17</sup> "Cyber Security Threat Modeling Based on the MITRE Enterprise ATT&CK Matrix | SpringerLink," no. 17, accessed August 14, 2022, <https://link.springer.com/article/10.1007/s10270-021-00898-7>.

<sup>18</sup> "Cyber Kill Chain®," Lockheed Martin, June 29, 2022, no. 18, <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.

military's "kill chain." The idea is to make network security teams aware of the 7 possible stages of a Cyber-attack, so they can understand the process and help them identify and stop an attack at each stage. The quicker they can detect and stop the bad actor during an attack the better they can defend their systems or delay an attack. In the paper from Kiwia et al<sup>19</sup> in 2018 they propose the Cyber Kill chain-based taxonomy of banking Trojans features. This threat intelligence-based taxonomy provides a stage-by-stage operational understanding of a cyber-attack and can be highly beneficial to security practitioners and inform the design of evolutionary computational intelligence on Trojans detection and mitigation strategy. The proposed taxonomy is built upon their analysis of a real-world dataset of 127 banking Trojans collected from December 2014 to January 2016 by a major UK-based financial organization.

#### ***H. ISO27001 monitoring and measuring***

ISO27001<sup>20</sup> is an information security management system. It's a security framework consisting of policies and procedures, including legal, physical and technical controls as part of an organizations information risk management processes. It helps organizations manage security risks to help in the fight against cyber-attacks, breaches, hacks or theft. Clause or chapter 9.1. of the ISO27001 measuring and monitoring<sup>21</sup> details the requirements of monitoring, measurement, analysis and evaluation.

---

<sup>19</sup> "Cyber Security Threat Modeling Based on the MITRE Enterprise ATT&CK Matrix | SpringerLink," no. 19.

<sup>20</sup> "ISO - ISO/IEC 27001 — Information Security Management," ISO, no. 20, accessed August 14, 2022, <https://www.iso.org/isoiec-27001-information-security.html>.

<sup>21</sup> "Measuring and Monitoring Your ISO 27001 ISMS," ICT Institute, March 10, 2022, no. 21, <https://ictinstitute.nl/measuring-and-monitoring-your-iso-27001-isms/>.



### III. RESEARCH METHODOLOGY

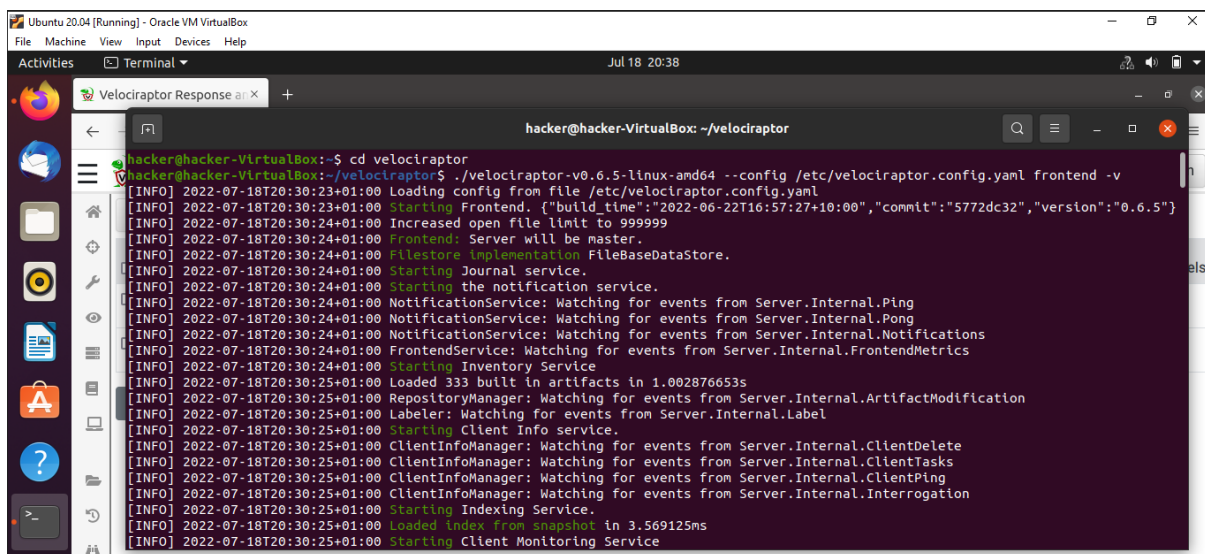
#### A. Approach

The purpose of this paper is to investigate a cyber threat group known as Cozy bear and the use of modern security tools to help defend against it. With a seemingly unlimited amount of information available, this author was able to form an understanding of the threat actors' methodology, targets, footprint, and ways to defend against it. According to CISA<sup>22</sup> the recent invasion of Russia in Ukraine could expose organizations both locally in Ukraine and outside to increased malicious cyber activity. Intelligence suggested that the Russian government had explored options for Cyber-attacks since the war began, which has been seen since March 2022. CISA highlights the different threat groups at the disposal of the Russian government and Cozy bear group is at the top of this list.

The approach was to configure a lab environment and install both defensive and threat hunting tools to simulate attack samples in how to stop Cozy bear.

#### B. Velociraptor

Once the author had configured the lab, the next step was to install the threat hunting tool known as Velociraptor. Full install instructions to install Velociraptor on Linux and Windows systems can be found here<sup>23</sup>. To start the Velociraptor frontend on the ubuntu machine you need to run the command `./velociraptor-v0.6.5-linux-amd64 --config /etc/velociraptor.config.yaml frontend -v` as in the below screen grab.



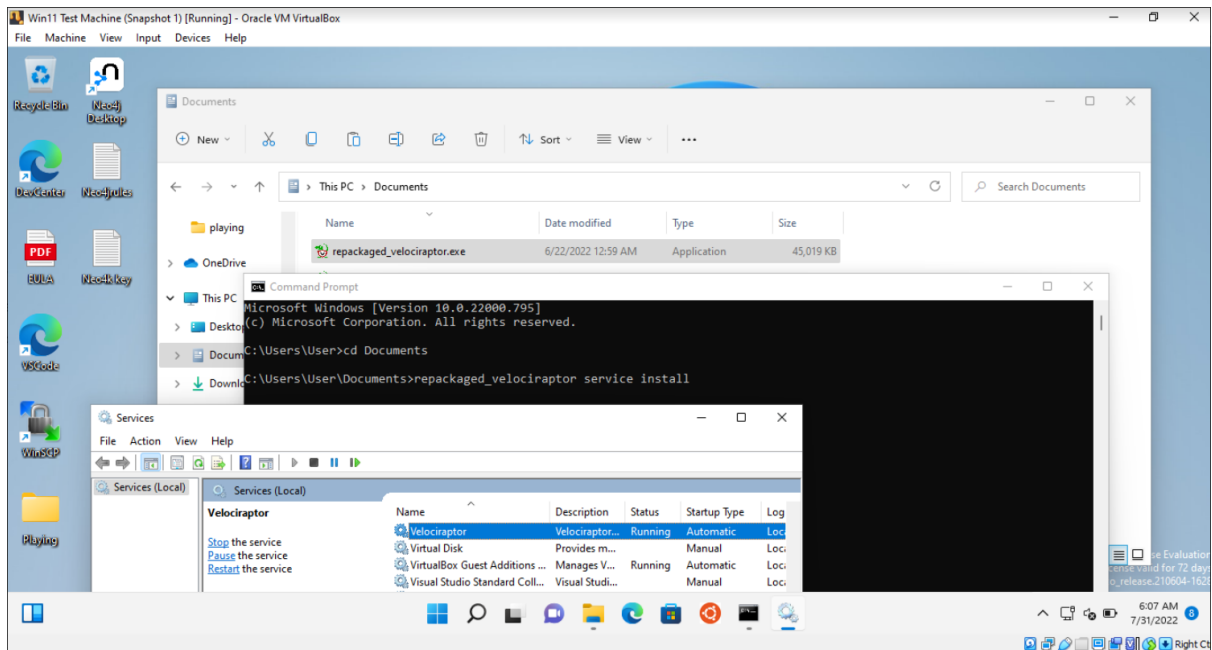
```
hacker@hacker-VirtualBox: ~/velociraptor
hacker@hacker-VirtualBox:~$ cd velociraptor
hacker@hacker-VirtualBox:~/velociraptor$ ./velociraptor-v0.6.5-linux-amd64 --config /etc/velociraptor.config.yaml frontend -v
[INFO] 2022-07-18T20:30:23+01:00 Loading config from file /etc/velociraptor.config.yaml
[INFO] 2022-07-18T20:30:23+01:00 Starting Frontend. {"build_time": "2022-06-22T16:57:27+10:00", "commit": "5772dc32", "version": "0.6.5"}
[INFO] 2022-07-18T20:30:24+01:00 Increased open file limit to 999999
[INFO] 2022-07-18T20:30:24+01:00 Frontend: Server will be master.
[INFO] 2022-07-18T20:30:24+01:00 Filestore Implementation FlleBaseDataStore.
[INFO] 2022-07-18T20:30:24+01:00 Starting Journal service.
[INFO] 2022-07-18T20:30:24+01:00 Starting the notification service.
[INFO] 2022-07-18T20:30:24+01:00 NotificationService: Watching for events from Server.Internal.Ping
[INFO] 2022-07-18T20:30:24+01:00 NotificationService: Watching for events from Server.Internal.Pong
[INFO] 2022-07-18T20:30:24+01:00 NotificationService: Watching for events from Server.Internal.Notifications
[INFO] 2022-07-18T20:30:24+01:00 FrontendService: Watching for events from Server.Internal.FrontendMetrics
[INFO] 2022-07-18T20:30:24+01:00 Starting Inventory Service
[INFO] 2022-07-18T20:30:25+01:00 Loaded 333 built in artifacts in 1.002876653s
[INFO] 2022-07-18T20:30:25+01:00 RepositoryManager: Watching for events from Server.Internal.ArtifactModification
[INFO] 2022-07-18T20:30:25+01:00 Labeler: Watching for events from Server.Internal.Label
[INFO] 2022-07-18T20:30:25+01:00 Starting Client Info service.
[INFO] 2022-07-18T20:30:25+01:00 ClientInfoManager: Watching for events from Server.Internal.ClientDelete
[INFO] 2022-07-18T20:30:25+01:00 ClientInfoManager: Watching for events from Server.Internal.ClientTasks
[INFO] 2022-07-18T20:30:25+01:00 ClientInfoManager: Watching for events from Server.Internal.ClientPing
[INFO] 2022-07-18T20:30:25+01:00 ClientInfoManager: Watching for events from Server.Internal.Interrogation
[INFO] 2022-07-18T20:30:25+01:00 Starting Indexing Service.
[INFO] 2022-07-18T20:30:25+01:00 Loaded Index from snapshot in 3.569125ms
[INFO] 2022-07-18T20:30:25+01:00 Starting Client Monitoring Service
```

Figure 1. Launching Velociraptor frontend

<sup>22</sup> "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA," no. 22, accessed August 14, 2022, <https://www.cisa.gov/uscert/ncas/alerts/aa22-110a>.

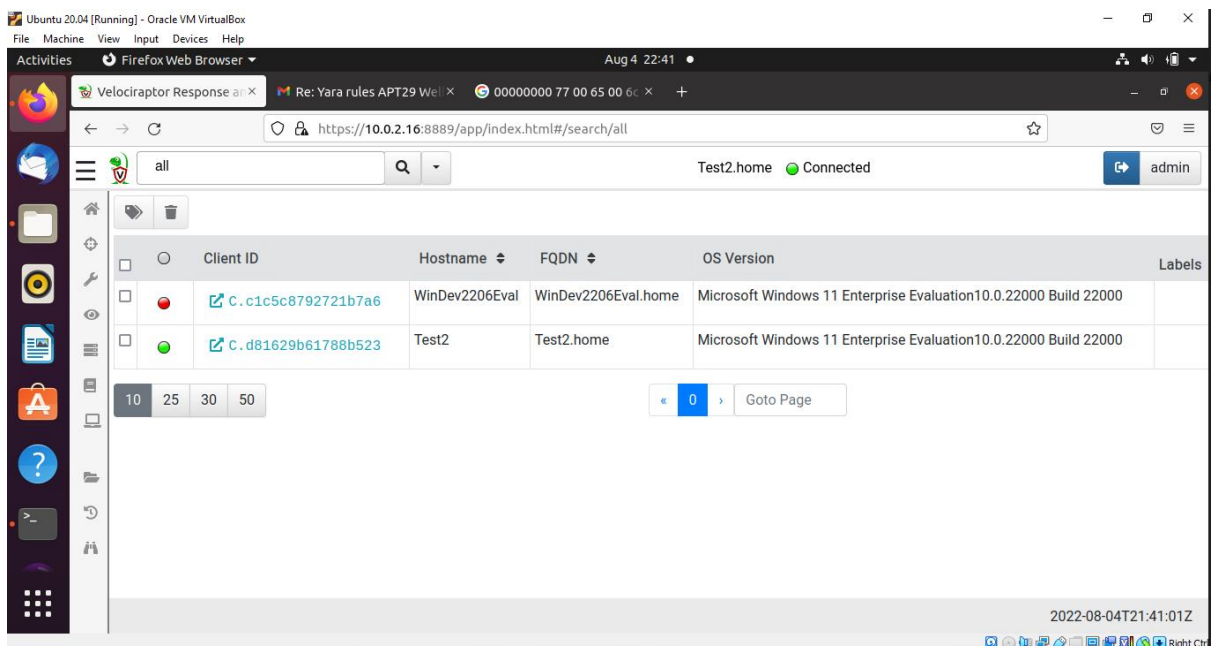
<sup>23</sup> cr00t, "Install Velociraptor Client on Linux and Windows Systems - Kifarunix.Com," January 8, 2021, no. 23, <https://kifarunix.com/install-velociraptor-client-on-linux-and-windows-systems/>.

With Velociraptor installed on an ubuntu 20.04 machine, next step was to install the Velociraptor service on the windows 11 machines setup in the environment. Using WinSCP or similar SFTP client to copy the repackaged Velociraptor exe file to windows to install as a service on each machine.



**Figure. 2.** Installing Velociraptor service on Windows

Once the service has been successfully installed, the client machine\’s should be visible from the Velociraptor browser window on the ubuntu machine as below. Ready for data to be collected and monitored from Velociraptor manager server for any malicious files that may be hidden on the Windows machines.



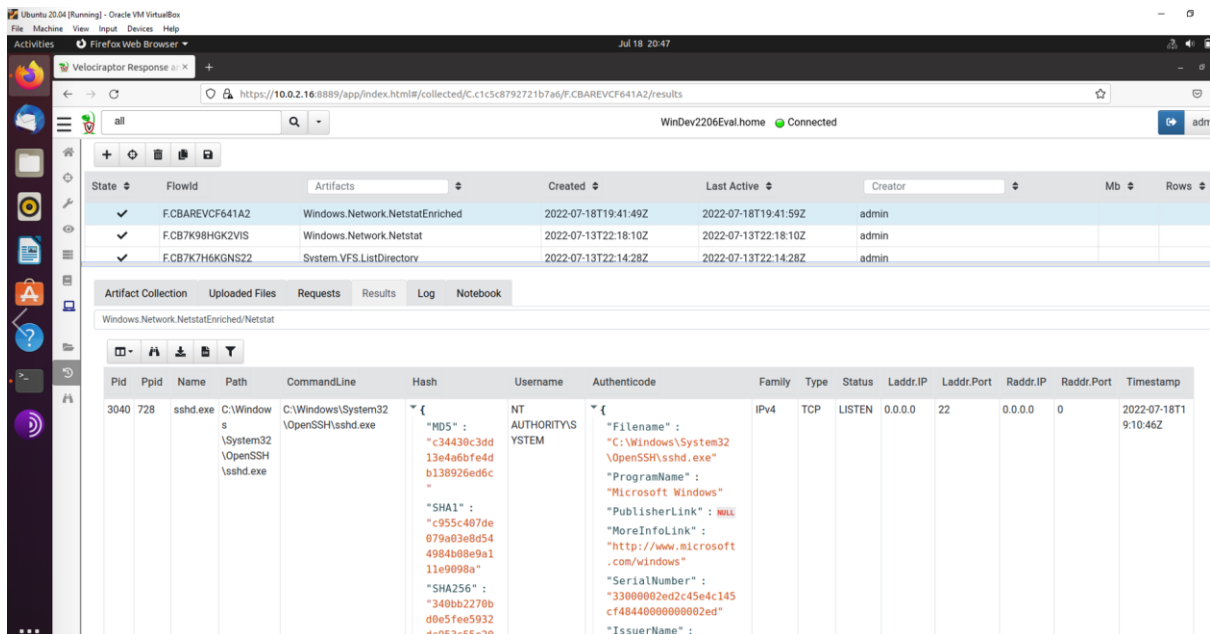
**Figure. 3.** Viewing connected machine in Velociraptor

## 1) Artifacts

### a) *Windows.Network.NetstatEnriched*

#### Displays:

- **Path** C:\Windows\System32\OpenSSH\sshd.exe
- **CommandLine**
- **Hash**
- **Authenticode signatures** - Authenticode is a **Microsoft code-signing technology that identifies the publisher of Authenticode-signed software**. Authenticode also verifies that the software has not been tampered with since it was signed and published. Authenticode uses cryptographic techniques to verify publisher identity and code integrity. Allows first responder to identify if a product is signed by a legitimate company. For example below I can see the ssh software under Authenticode is published by Microsoft, so can trust this program.



The screenshot shows the Velociraptor web interface. At the top, there is a table of artifacts with columns for State, Flowid, Artifacts, Created, Last Active, and Creator. The selected artifact is 'Windows.Network.NetstatEnriched' with flowid 'F.CBAREVCF641A2'. Below this, the 'Results' tab is active, showing a detailed view of the artifact. The table below contains the following data:

Pid	Ppid	Name	Path	CommandLine	Hash	Username	Authenticode	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr.IP	Raddr.Port	Timestamp
3040	728	sshd.exe	C:\Windows\System32\OpenSSH\sshd.exe	C:\Windows\System32\OpenSSH\sshd.exe	<pre>{   "MD5": "c34439c3dd13e4a6bfe4db138926ed6c",   "SHA1": "c955c407de079a03e8d544984b08e9a111e9098a",   "SHA256": "340bb2270bd0e5fee59324c053c55c10" }</pre>	NT AUTHORITY\SYSTEM	<pre>{   "Filename": "C:\Windows\System32\OpenSSH\sshd.exe",   "ProgramName": "Microsoft Windows",   "PublisherLink": null,   "MoreInfoLink": "http://www.microsoft.com/windows",   "SerialNumber": "3300002ed2c45e4c145cf484400000002ed",   "IssuerName": "" }</pre>	IPv4	TCP	LISTEN	0.0.0.0	22	0.0.0.0	0	2022-07-18T19:10:46Z

Figure. 4. Running Windows.Network.NetstatEnriched artifact

You can see the Velociraptor service and its issuer name details. So, as in this example below if you see an unsigned executable for example that looks suspicious you can investigate further.

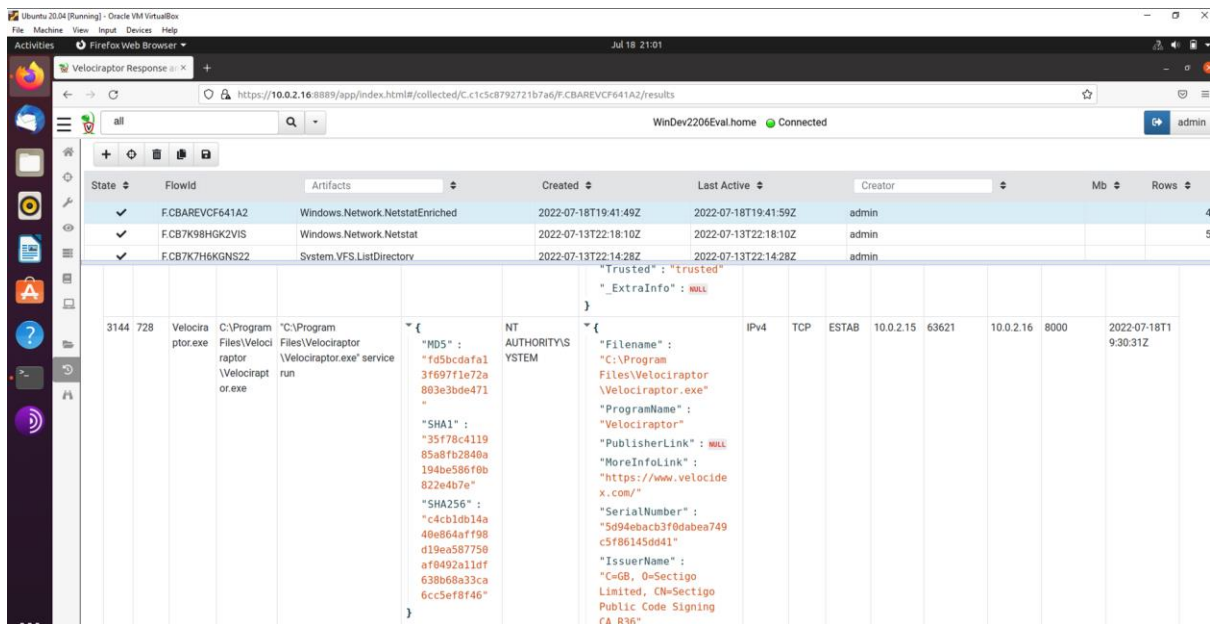


Figure. 5. Velociraptor service – issuer name

**b) Windows.Sysinternals.Autorun**

Suspecting one of the windows machines has been infected by Malware the first thing the author did here was to find out why something would launch automatically. We can run autoruns from the Velociraptor artifacts window below, autoruns is a Microsoft tool from Sysinternals. This will automatically download the tool onto the windows machine as in the case below and run it.

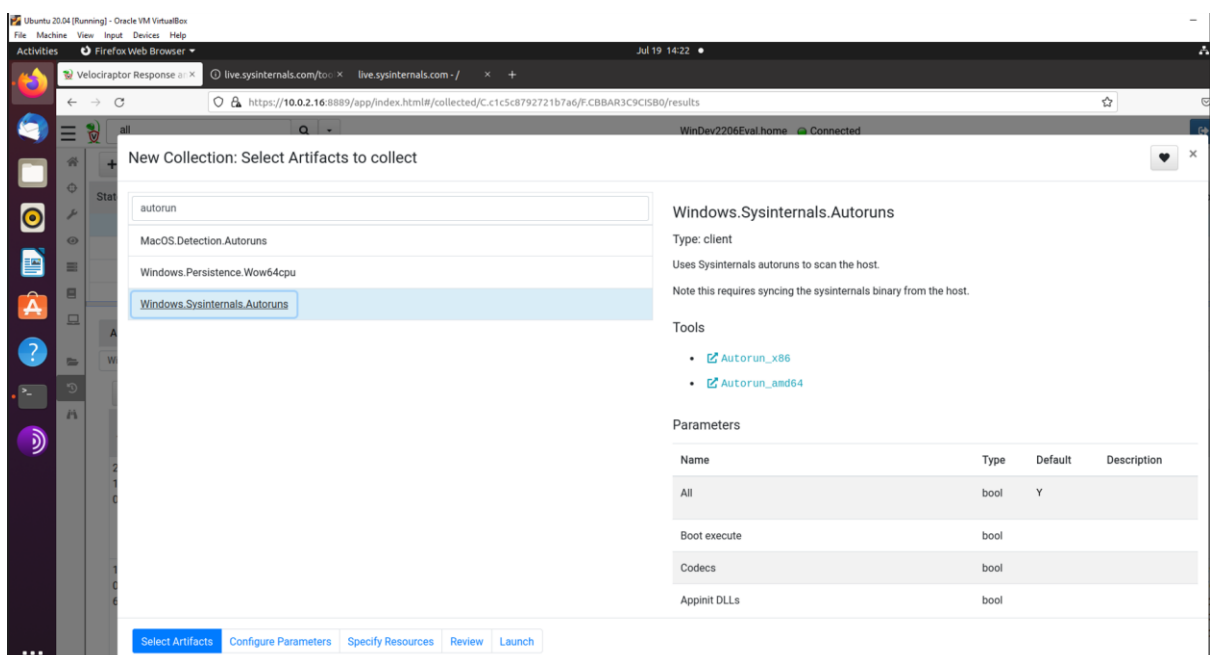


Figure. 6. Run Windows.Sysinternals.Autoruns artifact

A Sysinternals autoruns VQL query then generates the information below on the Velociraptor server from the windows 11 machine that the query was actioned against. As you can see it produces a lot of information in relation to services that run at start-up on the machine, below. This is helpful to a network defender in identifying if any malicious files have been added to the auto run process. In this example below it generated 1437 processes that run on start-up of this machine.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CBBAR3C9CISB0	Windows.Sysinternals.Autoruns	2022-07-19T13:11:41Z	2022-07-19T13:15:38Z	admin		1437
✓	F.CBAREVC64IA2	Windows.Network.NetstatEnriched	2022-07-18T19:41:49Z	2022-07-18T19:41:59Z	admin		43
✓	F.CB7K98HGK2VIS	Windows.Network.Netstat	2022-07-13T22:18:10Z	2022-07-13T22:18:10Z	admin		54
✓	F.CB7K7H6KGS22	System.VFS.ListDirectory	2022-07-13T22:14:28Z	2022-07-13T22:14:28Z	admin		1

Name	Path	Type	Status	Company
199305	HKLM\System\CurrentControlSet\Services\autocheck	System-wide	enabled	Microsoft Corporation
601	HKLM\System\CurrentControlSet\Services\autocheck *	System-wide	enabled	Microsoft Corporation
202206	HKLM\SOFTWARE\Classes\Hijacks	System-wide	enabled	Microsoft Corporation
18-055	HKLM\SOFTWARE\Classes\Hijacks	System-wide	enabled	Microsoft Corporation
07-182	HKLM\SOFTWARE\Classes\Hijacks	System-wide	enabled	Microsoft Corporation
311	HKLM\SOFTWARE\Classes\Hijacks	System-wide	enabled	Microsoft Corporation

Figure 7. Services that run on start-up

As this is not the easiest to search, there is an option to download the full list into an easy readable csv file as shown below. As you can see, it shows where each one is in the registry and if you scroll across to column H you can view which company signed this code. You can use information generated from autoruns to separate malware from the good stuff just by sorting by company. You can also see a description tab below to explain what each piece of software does.

Entry	Category	Profile	Description	Company
1	Enabled	Boot Execute	System-wide	Microsoft Corporation
2	enabled	Boot Execute	System-wide	Microsoft Corporation
3	enabled	Hijacks	System-wide	Microsoft Corporation
4	enabled	Hijacks	System-wide	Microsoft Corporation
5	enabled	Hijacks	System-wide	Microsoft Corporation
6	enabled	Services	System-wide	Microsoft Corporation
7	enabled	Services	System-wide	Microsoft Corporation
8	enabled	Services	System-wide	Microsoft Corporation
9	enabled	Services	System-wide	Microsoft Corporation
10	enabled	Services	System-wide	Microsoft Corporation
11	enabled	Services	System-wide	Microsoft Corporation
12	enabled	Services	System-wide	Microsoft Corporation
13	enabled	Services	System-wide	Microsoft Corporation
14	enabled	Services	System-wide	Microsoft Corporation
15	enabled	Services	System-wide	Microsoft Corporation
16	enabled	Services	System-wide	Microsoft Corporation
17	enabled	Services	System-wide	Microsoft Corporation
18	enabled	Services	System-wide	Microsoft Corporation
19	enabled	Services	System-wide	Microsoft Corporation
20	enabled	Services	System-wide	Microsoft Corporation
21	enabled	Services	System-wide	Microsoft Corporation
22	enabled	Services	System-wide	Microsoft Corporation
23	enabled	Services	System-wide	Microsoft Corporation
24	enabled	Services	System-wide	Microsoft Corporation
25	enabled	Services	System-wide	Microsoft Corporation
26	enabled	Services	System-wide	Microsoft Corporation
27	enabled	Services	System-wide	Microsoft Corporation
28	enabled	Services	System-wide	Microsoft Corporation
29	enabled	Services	System-wide	Microsoft Corporation
30	enabled	Services	System-wide	Microsoft Corporation
31	enabled	Services	System-wide	Microsoft Corporation
32	enabled	Services	System-wide	Microsoft Corporation
33	enabled	Services	System-wide	Microsoft Corporation
34	enabled	Services	System-wide	Microsoft Corporation
35	enabled	Services	System-wide	Microsoft Corporation
36	enabled	Services	System-wide	Microsoft Corporation
37	enabled	Services	System-wide	Microsoft Corporation
38	enabled	Services	System-wide	Microsoft Corporation
39	enabled	Services	System-wide	Microsoft Corporation
40	enabled	Services	System-wide	Microsoft Corporation
41	enabled	Services	System-wide	Microsoft Corporation

Figure 8. Extract to csv file



Autoruns stores any software without a signature at the bottom of the above list which makes it easier for a first responder to identify possible malware infection.

### c) *Windows.System.PSList*

Windows.System.Pslist can be used to find malware exe files on a machine.

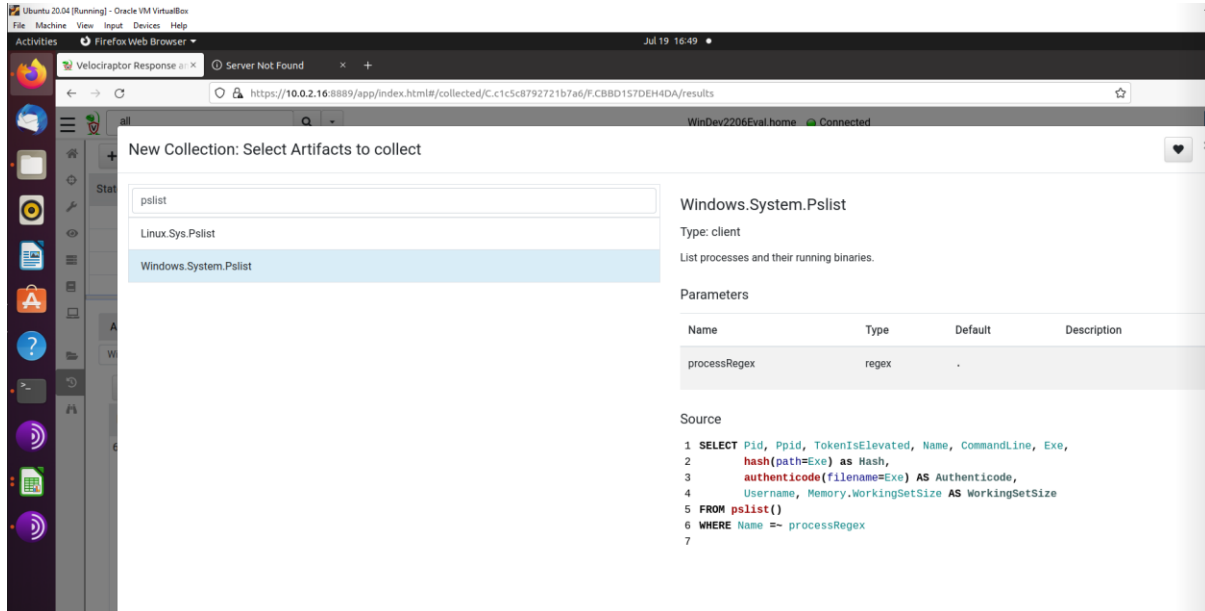


Figure 9. Run Windows.System.Pslist artifact

For this example below, the author installed an executable on one of the windows 11 machines that displays the 'Your machine is PWANED!' message when run.

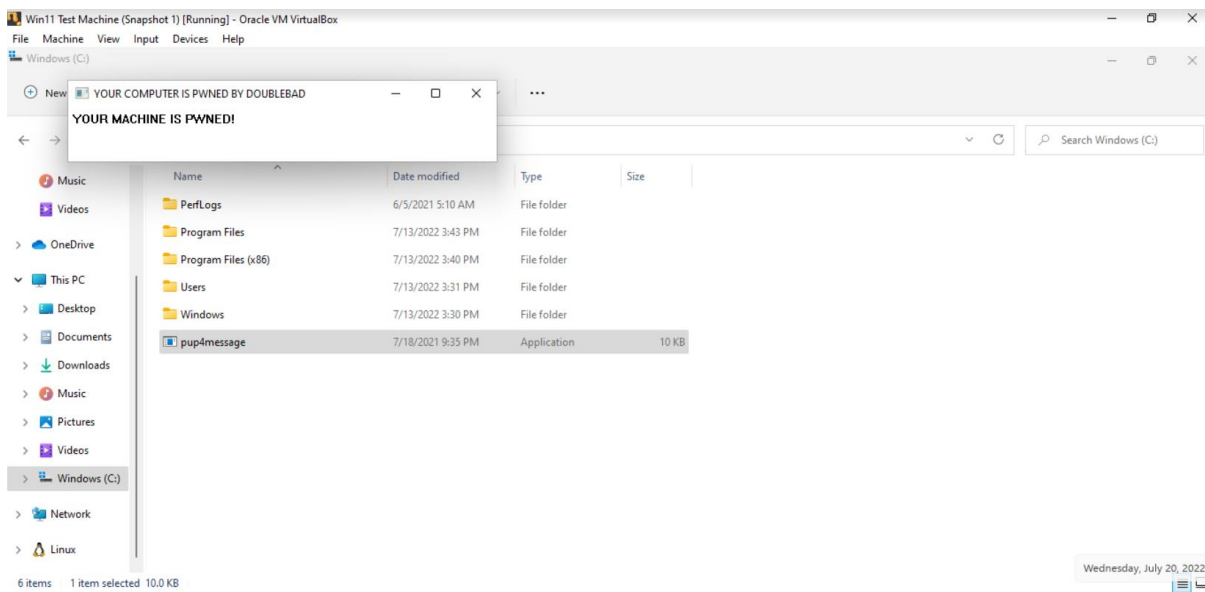


Figure 10. Run exe executable file on windows machine

Now to try and locate this file from my Velociraptor window control center. You can list all the processes or just give a string name as below to search for specific file name.

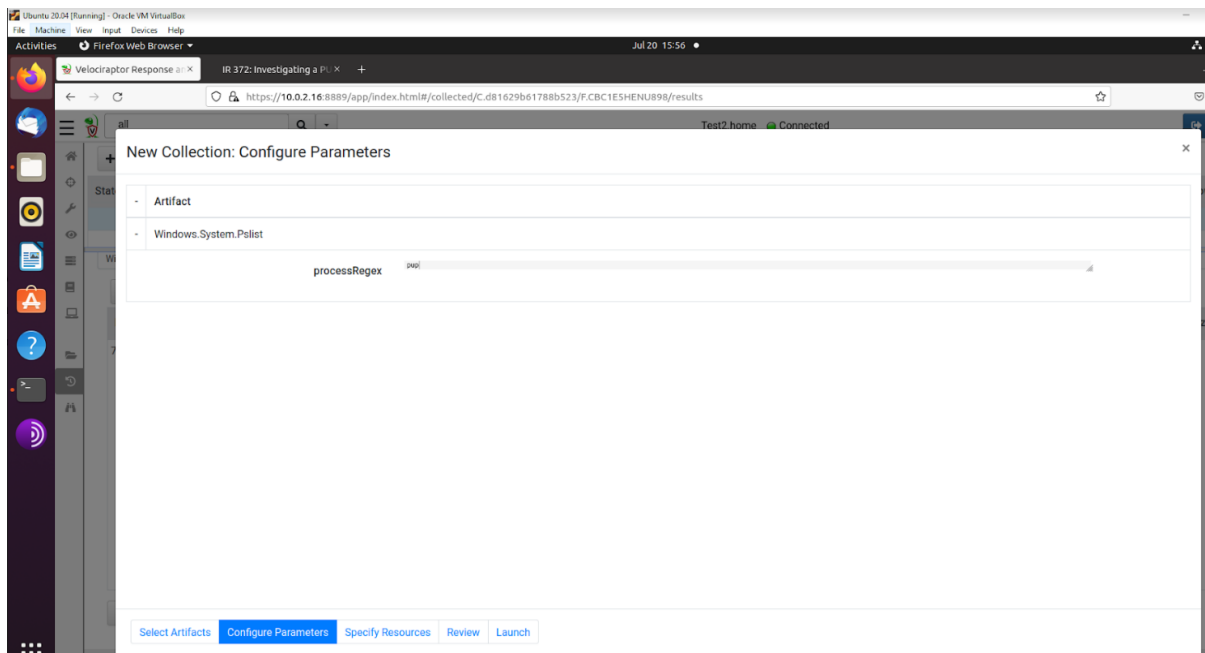


Figure. 11. Enter partial name of file for quicker search

Once Velociraptor returns results from the query, you can get information such as the hash (SHA256) of the found file which you can then analyse further.

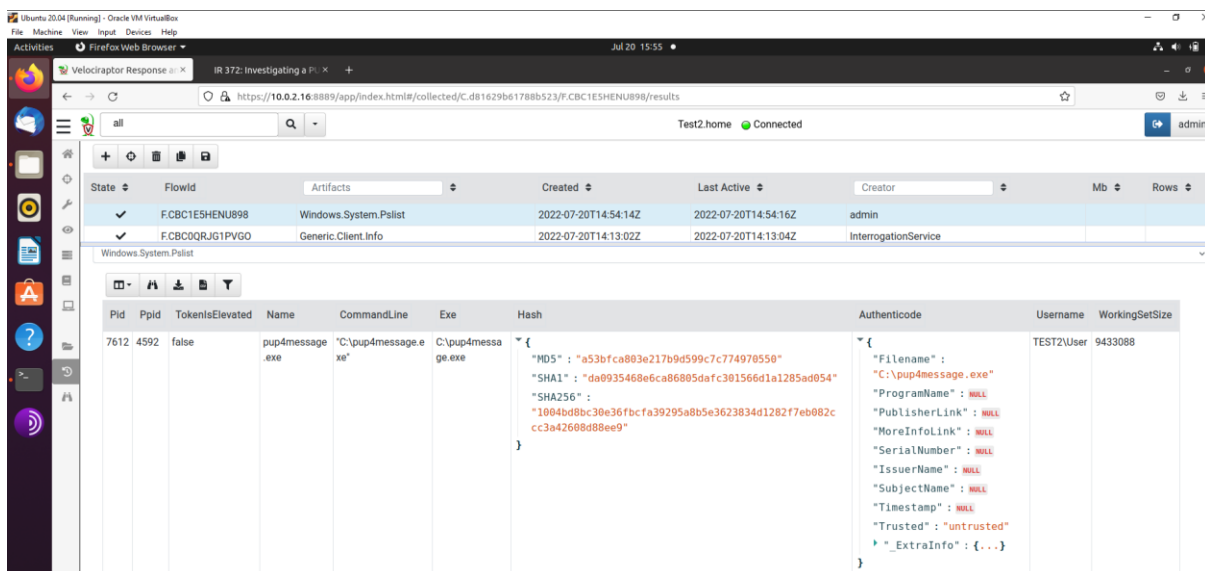


Figure. 12. Located file displaying hash information

#### d) *Windows.Triage.ProcessMemory*

The purpose of this step is to verify that the "pup4message" process is creating the pop-up message. Launch this collector: **Windows.Triage.ProcessMemory**

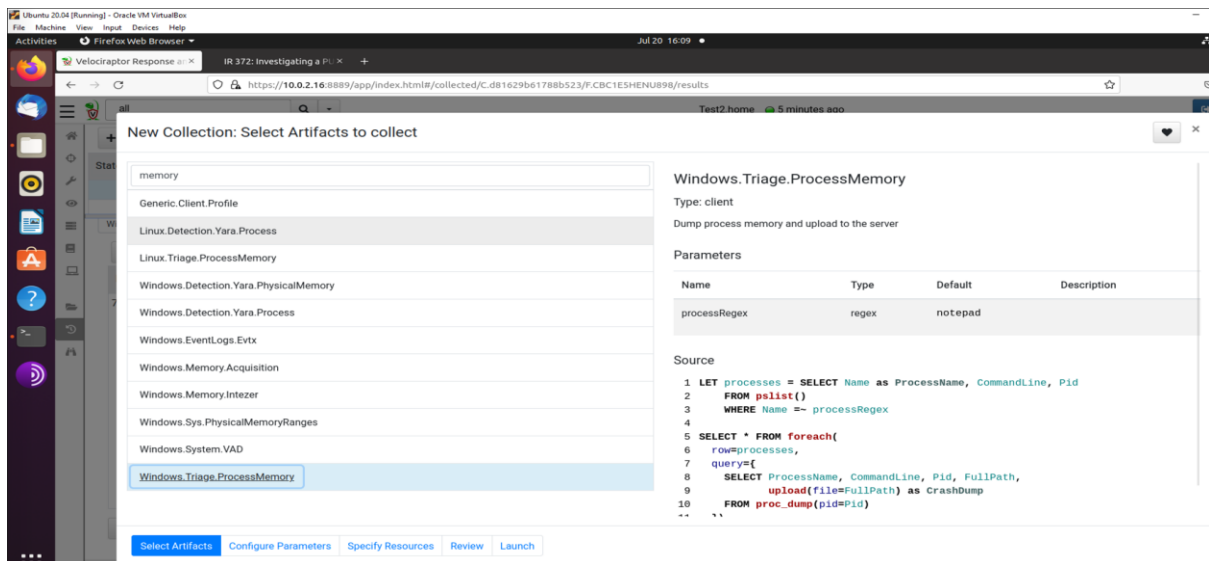


Figure. 13. Launch Windows.Triage.ProcessMemory artifact

Again to speed up the search I have altered the Windows.Triage.ProcessMemory artifact to part name of the suspicious file.

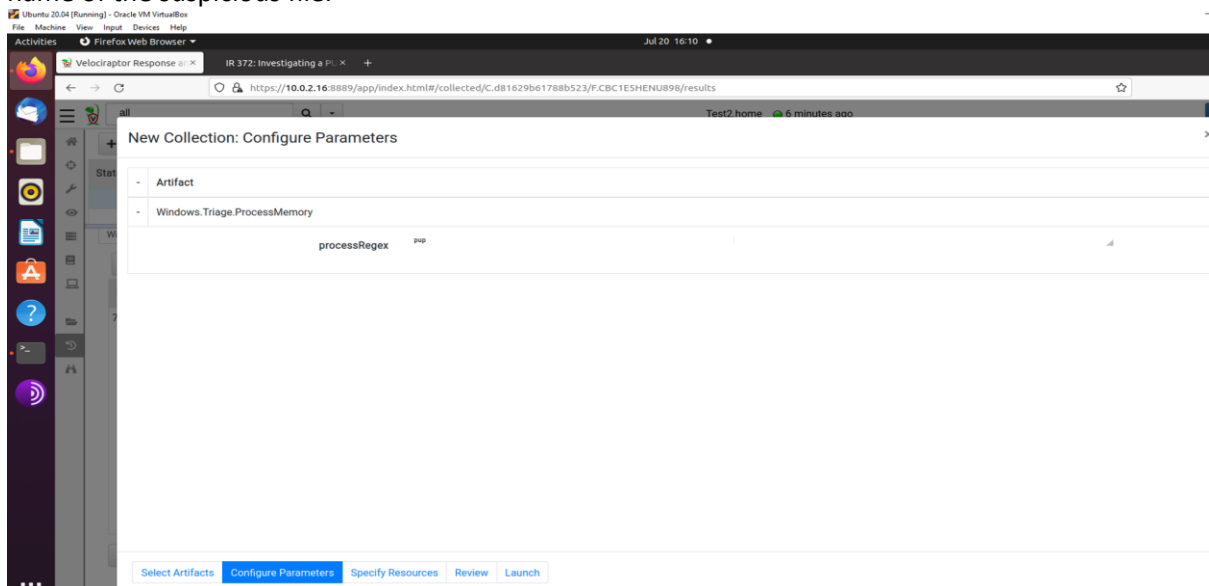
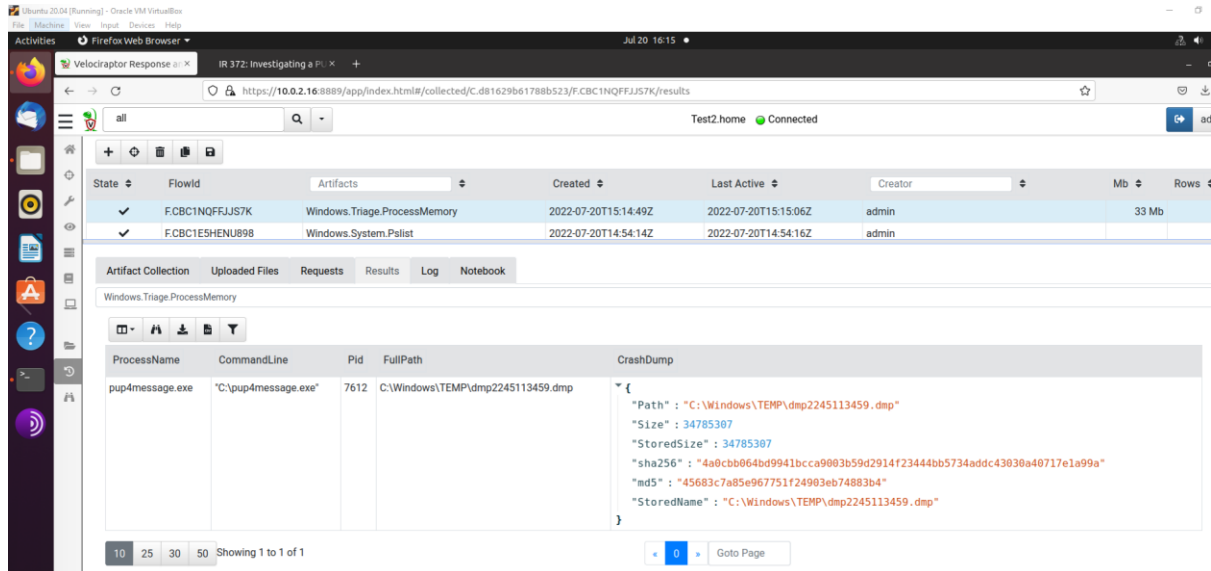


Figure. 14. Alter artifact search to locate file faster



## 2) Main Results

Similar information is displayed in the Velociraptor search window below as it finds the suspicious file, but with this search we can get a dmp file that we can extract and query further.



The screenshot shows the Velociraptor web interface in a Firefox browser. The main table displays search results for artifacts. Below the table, the details for the selected artifact 'Windows.Triage.ProcessMemory' are shown, including a table of process information and a JSON object for the crash dump.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	FCBC1NQFFJJS7K	Windows.Triage.ProcessMemory	2022-07-20T15:14:49Z	2022-07-20T15:15:06Z	admin		33 Mb
✓	FCBC1E5HENU898	Windows.System.Pollist	2022-07-20T14:54:14Z	2022-07-20T14:54:16Z	admin		

ProcessName	CommandLine	Pid	FullPath	CrashDump
pup4message.exe	"C:\pup4message.exe"	7612	C:\Windows\TEMP\dmp2245113459.dmp	{ "Path" : "C:\Windows\TEMP\dmp2245113459.dmp" "Size" : 34785307 "StoredSize" : 34785307 "sha256" : "4a0cb064b09941bcca9003b59d2914f23444bb5734addc43030a40717e1a99a" "md5" : "45683c7a85e967751f24903eb74883b4" "StoredName" : "C:\Windows\TEMP\dmp2245113459.dmp" }

**Figure. 15.** Results of suspicious file displayed

There is an online sharing community that allows users of Velociraptor to get access to other queries that may assist their needs or allow them to post queries they have created themselves.

### C. PEStudio

In the example below the author was able to safely download a copy of the Wellmess malware used by the Cozybear group in attack campaigns seen in the wild in 2021. Note, this is done in a controlled environment using a VPN and TOR browser. PEStudio<sup>24</sup> is a free tool to allow security professionals to perform an initial assessment of a malware without infecting a system or studying its code, simply by drag and dropping the malicious file into the PEStudio window.

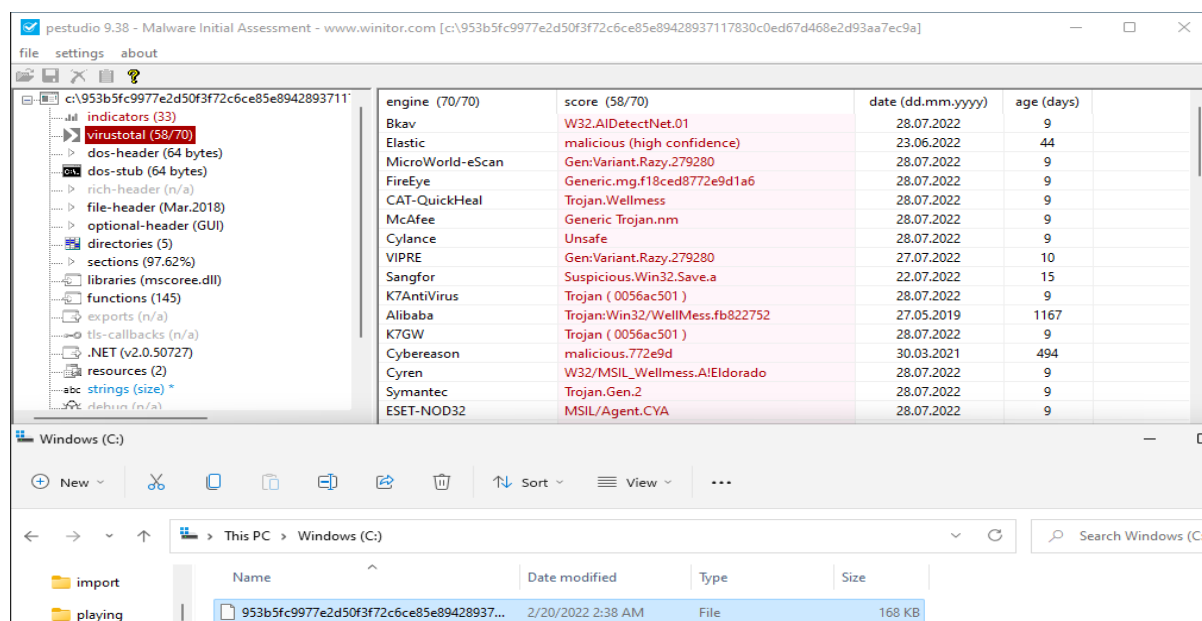


Figure 16. PEStudio to assess Wellmess malware

Hash: 953b5fc9977e2d50f3f72c6ce85e89428937117830c0ed67d468e2d93aa7ec9a

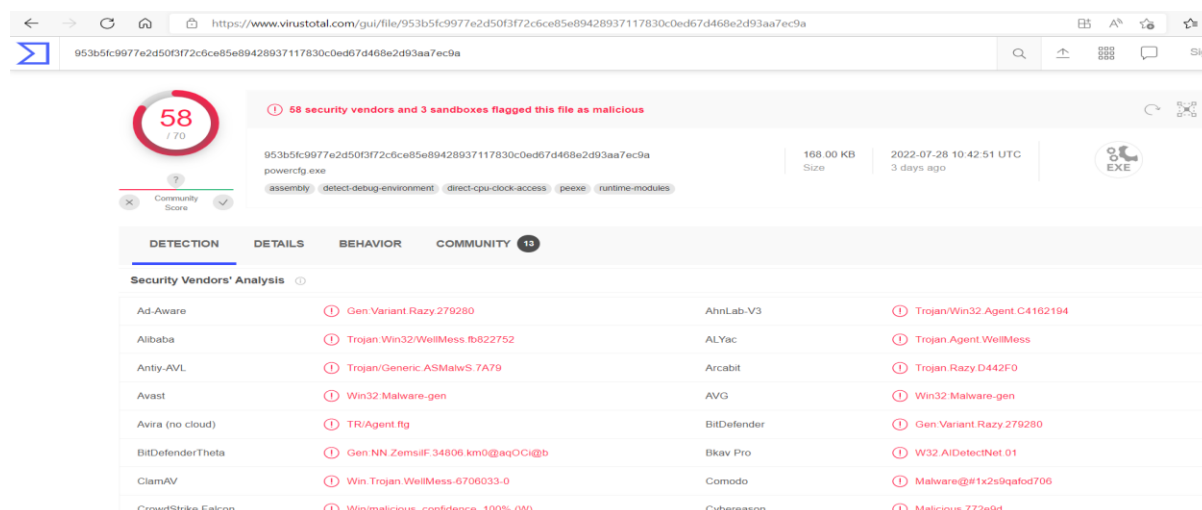


Figure 17. Wellmess malware security vendors rating

<sup>24</sup> Mirko Zorz, "Pestudio: Initial Malware Assessment Made Simple," *Help Net Security* (blog), June 16, 2016, no. 24, <https://www.helpnetsecurity.com/2016/06/16/pestudio-initial-malware-assessment/>.

## 1) Yara

Yara<sup>25</sup> is another very useful tool to help in detecting malware. Below is a Yara rule to detect strings in relation to the Wellmess malware. When run against the version of Wellmess this author was able to download from the web, you can see in the command prompt window that it does detect 5 out of the 6 strings used in the Yara rule below.

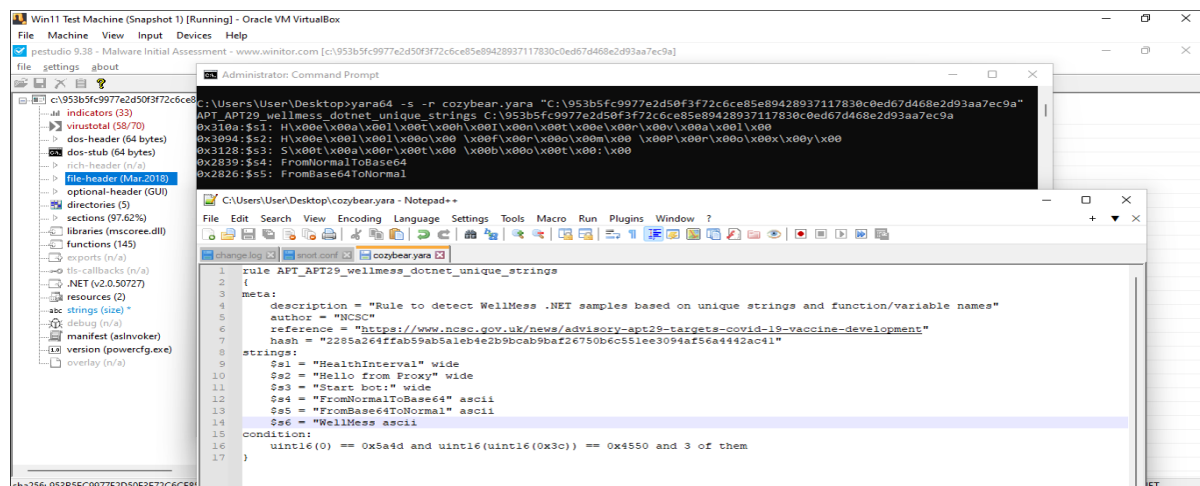


Figure 18. Yara rule to run against malware

## D. Hayabusa Tool

Hayabusa<sup>26</sup> is a Windows event log tool used to allow fast forensics of event logs for threat hunting. It has over 2400 Sigma rules and 130 built-in detection rules with many more being added on a regular basis. For this research paper the author ran it locally on a windows 11 machine, but it can also be used in conjunction with Velociraptor when imported as an artifact and the query ran from there. Once installed it can be run as below from the command prompt in Windows.

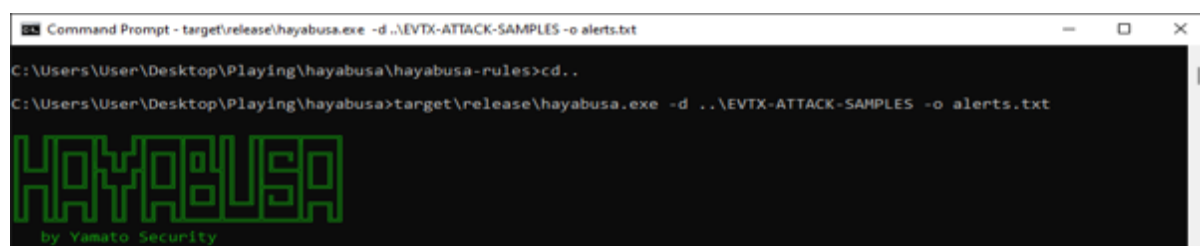


Figure 19. Launch Hayabusa against Attack samples

Hayabusa can identify 371 unique detections here with 12 labelled critical in a matter of seconds. The command used above then generates a txt file with the detection records broken down into labels as shown on the below.

<sup>25</sup> "YARA: Effective Tool to Detect Malware," no. 25, accessed August 14, 2022, <https://www.cyber.nj.gov/informational-report/yara-effective-tool-to-detect-malware>.

<sup>26</sup> "About Hayabusa," Rust (2020; repr., Yamato Security 大和セキュリティ, August 14, 2022), no. 26, <https://github.com/Yamato-Security/hayabusa>.

```

Command Prompt
Total informational detections: 3176
Unique detections: 371
Unique critical detections: 12
Unique high detections: 170
Unique medium detections: 98
Unique low detections: 51
Unique informational detections: 40

Date with most total critical detections: 2019-07-19 (10)
Date with most total high detections: 2019-05-18 (249)
Date with most total medium detections: 2019-07-19 (93)
Date with most total low detections: 2019-04-30 (135)
Date with most total informational detections: 2019-03-18 (901)

Top 5 computers with most unique critical detections: MSEDGWIN10 (6), IEWIN7 (3), DESKTOP-PIU87N6 (1), alice.insecurebank.local (1), DC1.insecurebank.local (1)
Top 5 computers with most unique high detections: MSEDGWIN10 (104), IEWIN7 (64), LAPTOP-JU4M3I0E (12), PC01.example.corp (12), PC04.example.corp (10)
Top 5 computers with most unique medium detections: MSEDGWIN10 (62), IEWIN7 (33), PC01.example.corp (13), LAPTOP-JU4M3I0E (12), 01566s-win16-ir.threebeesco.com (5)
Top 5 computers with most unique low detections: MSEDGWIN10 (36), IEWIN7 (18), LAPTOP-JU4M3I0E (9), PC01.example.corp (6), alice.insecurebank.local (4)
Top 5 computers with most unique informational detections: MSEDGWIN10 (19), IEWIN7 (17), PC01.example.corp (13), WIN-77LTAPHIQ1R.example.corp (9), 01566s-win16-ir.threebeesco.com (8)

Elapsed Time: 00:01:06.829
C:\Users\User\Desktop\Playing\havabusa>

```

Figure. 20. Results detected from scan

### 1) Main Results

As you can see below each of the items detected is then labelled to show the user labels such as timestamp, computer, event ID, MitreAttack and so on.

```

Win11 Test Machine (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
alerts - Notepad
File Edit View

|Timestamp,Computer,Channel,EventID,Level,MitreAttack,RecordID,RuleTitle,Details,RuleFile,EvtxFile
2017-06-09 12:21:26.968 -07:00,2016dc.hqcorp.local,Sec,4794,high,Persis,3139859,Password Change on Directory Service Restore Mode (DSRM) Acc
2017-06-12 16:39:43.512 -07:00,2012r2srv.maincorp.local,Sec,4765,med,Persis | PrivEsc,8075,Addition of SID History to Active Directory Objec
2019-01-19 05:00:10.350 -08:00,IEWIN7,Sec,5145,info,Collect,84038,NetShare File Access,User: IEUser | ShareName: \\*\ADMIN$ | SharePath: \??
2019-01-19 05:00:10.350 -08:00,IEWIN7,Sec,5145,info,Collect,84039,NetShare File Access,User: IEUser | ShareName: \\*\ADMIN$ | SharePath: \??
2019-01-19 05:00:10.548 -08:00,IEWIN7,Sec,5145,high,LatMov,84047,First Time Seen Remote Named Pipe,User: IEUser | ShareName: \\*\IPC$ | Share
2019-01-19 05:00:10.711 -08:00,IEWIN7,Sec,5145,high,LatMov,84050,First Time Seen Remote Named Pipe,User: IEUser | ShareName: \\*\IPC$ | Share
2019-01-19 05:00:10.711 -08:00,IEWIN7,Sec,5145,high,LatMov,84051,First Time Seen Remote Named Pipe,User: IEUser | ShareName: \\*\IPC$ | Share
2019-01-19 05:00:10.711 -08:00,IEWIN7,Sec,5145,high,LatMov,84050,Suspicious PsExec Execution,User: IEUser | ShareName: \\*\IPC$ | SharePath:
2019-01-19 05:00:10.711 -08:00,IEWIN7,Sec,5145,high,LatMov,84051,Suspicious PsExec Execution,User: IEUser | ShareName: \\*\IPC$ | SharePath:
2019-01-19 05:00:10.711 -08:00,IEWIN7,Sec,5145,high,LatMov,84052,Suspicious PsExec Execution,User: IEUser | ShareName: \\*\IPC$ | SharePath:
2019-01-19 05:00:10.711 -08:00,IEWIN7,Sec,5145,high,LatMov,84052,First Time Seen Remote Named Pipe,User: IEUser | ShareName: \\*\IPC$ | Share
2019-01-19 23:00:50.800 -08:00,WIN-77LTAPHIQ1R.example.corp,Sec,1102,high,Evas,32853,Security Log Cleared,User: Administrator,Sec_1102_Secur
2019-01-19 23:29:57.863 -08:00,WIN-77LTAPHIQ1R.example.corp,Sec,1102,high,Evas,32950,Security Log Cleared,User: Administrator,Sec_1102_Secur
2019-02-02 01:16:52.479 -08:00,ICORP-DC.internal.corp,Sec,4776,info,,65966,NTLM Logon To Local Account,User: helpdesk | Comp: evil.internal.c
2019-02-02 01:17:22.562 -08:00,ICORP-DC.internal.corp,Sec,4776,info,,65968,NTLM Logon To Local Account,User: EXCHANGE$ | Comp: EXCHANGE | St
2019-02-02 01:17:22.563 -08:00,ICORP-DC.internal.corp,Sec,4624,info,,65969,Logon (Type 3 Network),User: EXCHANGE$ | Comp: EXCHANGE | IP-Addr
2019-02-02 01:17:22.563 -08:00,ICORP-DC.internal.corp,Sec,4624,med,LatMov,65969,Pass the Hash Activity 2,User: EXCHANGE$ | Comp: EXCHANGE | :
2019-02-02 01:17:27.629 -08:00,ICORP-DC.internal.corp,Sec,5136,info,,65972,Dir Svc Obj Modified,"Operation: %%%14675 | DN: DC=internal,DC=corp
2019-02-02 01:17:27.629 -08:00,ICORP-DC.internal.corp,Sec,5136,high,Persis,65972,Powerview Add-DomainObjectAcl DCSync AD Extend Right,"User:
2019-02-02 01:17:27.629 -08:00,ICORP-DC.internal.corp,Sec,5136,info,,65973,Dir Svc Obj Modified,"Operation: %%%14674 | DN: DC=internal,DC=corp
2019-02-02 01:17:27.629 -08:00,ICORP-DC.internal.corp,Sec,5136,high,Persis,65973,Powerview Add-DomainObjectAcl DCSync AD Extend Right,"User:
2019-02-13 07:15:04.175 -08:00,PC02.example.corp,Sec,4624,info,,5281,Logon (Type 0 System),Bootup,Sec_4624_Logon-Type-0-System.yml, .\EVTX-A
2019-02-13 07:15:08.689 -08:00,PC02.example.corp,Sec,4624,low,,5299,Logon (Type 5 Service),User: sshd_server | Comp: PC02 | IP-Addr: - | LID
2019-02-13 07:19:51.259 -08:00,PC02.example.corp,Sec,4624,info,,5308,Logon (Type 2 Interactive) *Credentials stored in memory*,User: IEUser
2019-02-13 07:26:53.356 -08:00,PC02.example.corp,Sec,4624,info,,5315,Logon (Type 10 RemoteInteractive (RDP)) *Credentials in memory*,User: I
2019-02-13 07:26:53.356 -08:00,PC02.example.corp,Sec,4624,high,LatMov,5315,RDP Login from Localhost,User: IEUser | Comp: PC02 | IP-Addr: 127
2019-02-13 07:29:40.657 -08:00,PC02.example.corp,Sec,4624,info,,5319,Logon (Type 2 Interactive) *Credentials stored in memory*,User: IEUser
2019-02-13 07:31:19.529 -08:00,PC02.example.corp,Sec,4624,info,,5322,Logon (Type 3 Network),User: ANONYMOUS LOGON | Comp: PC01 | IP-Addr: 10
2019-02-13 07:31:31.556 -08:00,PC02.example.corp,Sec,4624,info,,5323,Logon (Type 3 Network),User: ANONYMOUS LOGON | Comp: PC01 | IP-Addr: 10
2019-02-13 10:01:41.593 -08:00,PC01.example.corp,Sec,1102,high,Evas,227693,Security Log Cleared,User: admin01,Sec_1102_SecurityLogCleared.yml
2019-02-13 10:01:47.562 -08:00,PC01.example.corp,Sec,4688,info,,227695,Proc Exec,CmdLine: | Path: C:\Windows\System32\TSTheme.exe | PID: 0x:
2019-02-13 10:02:04.426 -08:00,PC01.example.corp,Sec,4624,info,,227701,Logon (Type 11 CachedInteractive) *Credentials in memory*,User: user0:
2019-02-13 10:02:04.426 -08:00,PC01.example.corp,Sec,4648,info,PrivEsc | LatMov,227700,Explicit Logon,SrcUser: PC01$ | TgtUser: user01 | IP-:
2019-02-13 10:02:04.526 -08:00,PC01.example.corp,Sec,4624,info,,227708,Logon (Type 7 Unlock),User: user01 | Comp: PC01 | IP-Addr: - | LID: 0:
2019-02-13 10:02:04.526 -08:00,PC01.example.corp,Sec,4648,info,PrivEsc | LatMov,227707,Explicit Logon,SrcUser: PC01$ | TgtUser: user01 | IP-:
2019-02-13 10:02:05.528 -08:00,PC01.example.corp,Sec,4688,info,,227712,Proc Exec,CmdLine: | Path: C:\Windows\System32\AtBroker.exe | PID: 0:
2019-02-13 10:03:28.318 -08:00,PC01.example.corp,Sec,4688,info,,227714,Proc Exec,CmdLine: | Path: C:\Users\User01\Desktop\plink.exe | PID: 0:
Ln 1, Col 1 100% Unix (LF) UTF-8

```

Figure. 21. CSV file of detections

Critical alerts extracted from the file above:

Computer	Level	Rule	Title
IEWIN7	critical	Malicious	Named Pipe
IEWIN7	critical	CobaltStrike	Service Installations in Registry
DC1.insecurebank.local	critical	Active Directory Replication	from Non Machine Account
IEWIN7	critical	Meterpreter or Cobalt Strike	Getsystem Service Installation
alice.insecurebank.local	critical	Dumpert	Process Dumper
MSEDGEWIN10	critical	Windows Defender	Alert
MSEDGEWIN10	critical	WannaCry	Ransomware
MSEDGEWIN10	critical	Sticky Key	Like Backdoor Usage
MSEDGEWIN10	critical	TrustedPath	UAC Bypass Pattern
MSEDGEWIN10	critical	Mimikatz	MemSSP Default Log File Creation
DESKTOP-PIU87N6	critical	Suspicious	LSASS Process Clone
MSEDGEWIN10	critical	Suspicious	LSASS Process Clone

Figure. 22. Critical detections

### E. Neo4j

In the event of thousands of detections being identified it could make searching for critical events slow and cumbersome. In this lab to combat this the author installed Neo4j desktop<sup>27</sup> is graph database that can work with Highly connected data to allow users to map, store and traverse networks to reveal invisible contents and hidden relationships. For this paper it was used to map unique detections that Hayabusa was able to locate when querying the EVTX-Attack-Samples and provide a graphical interface to view critical and suspicious files easily and quickly.

The txt alert file generated on the previous page via Hayabusa can now be imported into Neo4j to allow a user to query it to generate a graphical view of all detections to allow a user a clear view of any suspicious or critical alerts in a user-friendly database.

```
//CREATE Host Constraint
CREATE CONSTRAINT host_name IF NOT EXISTS
FOR (n:Host)
REQUIRE n.name IS UNIQUE

//CREATE Alert Constraint
CREATE CONSTRAINT alert_name IF NOT EXISTS
FOR (n:Alert)
REQUIRE n.name IS UNIQUE
// Load Data
LOAD CSV WITH HEADERS FROM 'file:///playing/alerts-transform1.txt' AS row
MERGE (a:Alert{name:row.RuleTitle})
MERGE (h:Host{name:row.Computer})
MERGE (a)-[:Serverity{level: row.Level}]->(h)
```

<sup>27</sup> "Neo4j Desktop - Neo4j Browser," Neo4j Graph Data Platform, no. 27, accessed August 14, 2022, <https://neo4j.com/docs/browser-manual/4.4/deployment-modes/neo4j-desktop/>.

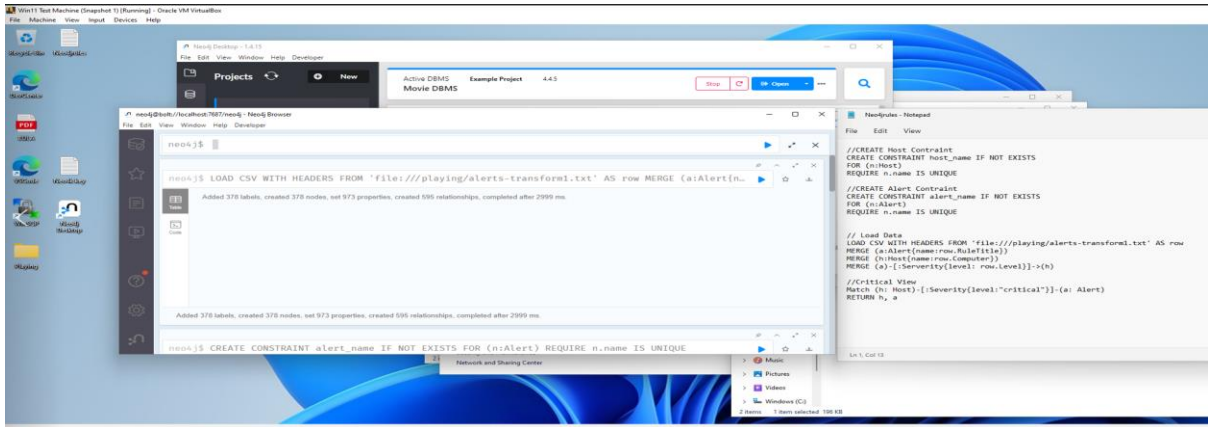


Figure. 23. Query commands entered in the Neo4j Database

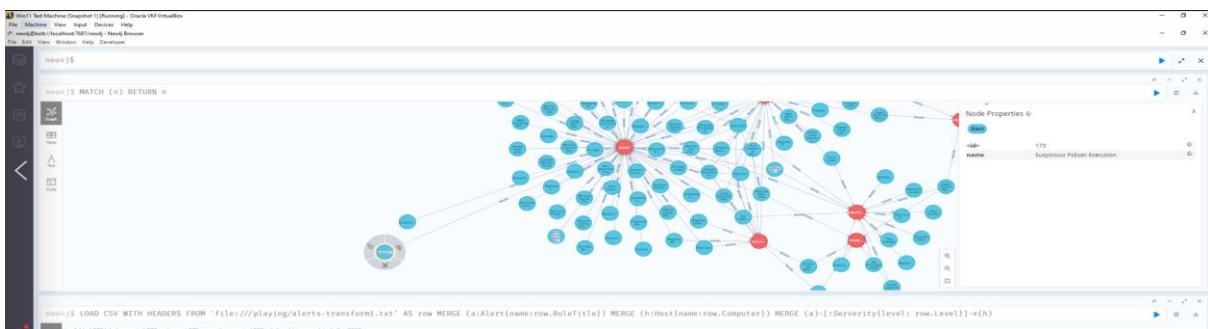


Figure. 24. Neo4j graphical results

To narrow the search to only show critical alerts the user can enter the following code into the neo4j run window at the top of the screen, selecting the run button to get the graphical window below. This makes Threat hunting for Cozy bear files and similar easier for network defenders.

```
//Critical View
MATCH (h: Host)-[:Severity{level:"critical"}]->(a: Alert)
RETURN h, a
```

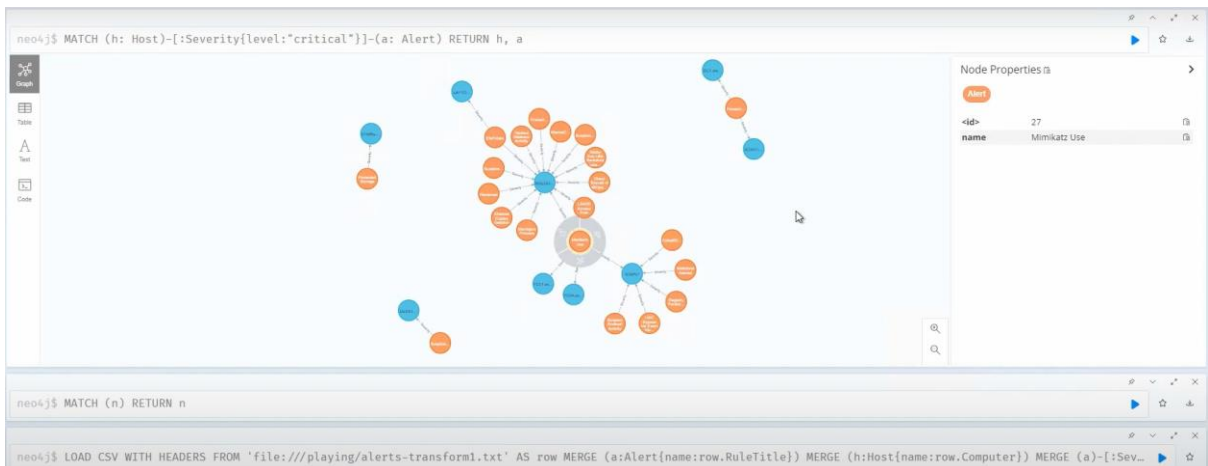
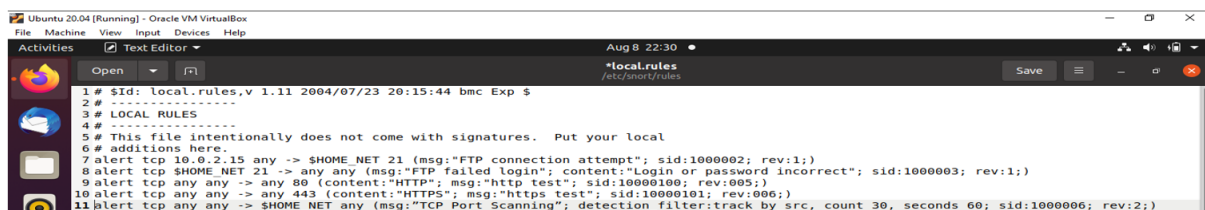


Figure. 25. Critical detections visible in Neo4j



## F. Snort Tool

Snort is an intrusion detection system to help detect suspicious or unacceptable system and network activity and to alert systems administrators of this activity. IDS systems generally use a set of signatures that define what suspicious traffic is. The aim of the organization that developed Snort is to identify a way in which it could be developed further by generalising rules to identify novel attacks according to Aickelin et al<sup>28</sup> in 2007. TTPs otherwise known as **Tactics, Techniques, and Procedures** in relation to Cozy bear have as stated by the National Cyber Security Centre in the UK<sup>29</sup> suggest a number of Snort alert rules to be added to the local.rules files of network defenders Snort configuration to help detect signatures of Wellmess or Sliver as its also been known attack threats, as shown below. A Port scanning detection alert is also added to detect NMAP Port scanning.

A screenshot of a text editor window titled 'local.rules' showing Snort configuration rules. The rules are numbered 1 through 11. Rule 7 is an alert for FTP connection attempts. Rule 8 is an alert for FTP failed logins. Rule 9 is an alert for HTTP tests. Rule 10 is an alert for HTTPS tests. Rule 11 is an alert for TCP port scanning, with a detection filter to track by source IP, count 30, and seconds 60.

```
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # -----
3 # LOCAL RULES
4 # -----
5 # This file intentionally does not come with signatures.  Put your local
6 # additions here.
7 alert tcp 10.0.2.15 any -> $HOME_NET 21 (msg:"FTP connection attempt"; sid:1000002; rev:1;)
8 alert tcp $HOME_NET 21 -> any any (msg:"FTP failed login"; content:"Login or password incorrect"; sid:1000003; rev:1;)
9 alert tcp any any -> any 80 (content:"HTTP"; msg:"http test"; sid:10000100; rev:005;)
10 alert tcp any any -> any 443 (content:"HTTPS"; msg:"https test"; sid:10000101; rev:006;)
11 alert tcp any any -> $HOME_NET any (msg:"TCP Port Scanning"; detection_filter:track by_src, count 30, seconds 60; sid:1000006; rev:2;)
```

Figure. 26. Local.rules file

The author ran an Nmap<sup>30</sup> scan from one of the windows machines in this lab targeting the ubuntu machine, as an example to reflect an attacker’s scan which can be seen on the next page.

<sup>28</sup> Uwe Aickelin, Jamie Twycross, and Thomas Hesketh-Roberts, “Rule Generalisation in Intrusion Detection Systems Using SNORT,” *International Journal of Electronic Security and Digital Forensics* 1, no. 1 (January 2007): no. 28, <https://doi.org/10.1504/IJESDF.2007.013596>.

<sup>29</sup> “Advisory Further TTPs Associated with SVR Cyber Actors.Pdf,” no. 29, accessed August 14, 2022, <https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf>.

<sup>30</sup> “Chapter 11. Defenses Against Nmap | Nmap Network Scanning,” no. 30, accessed August 14, 2022, <https://nmap.org/book/defenses.html>.

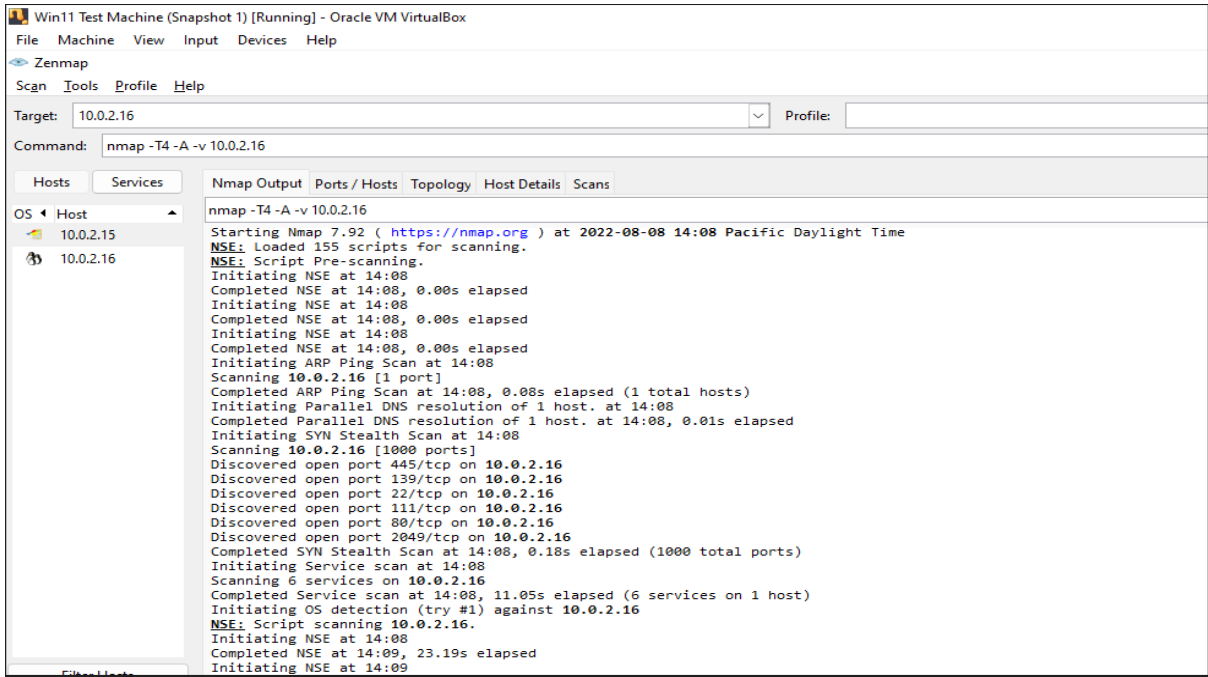
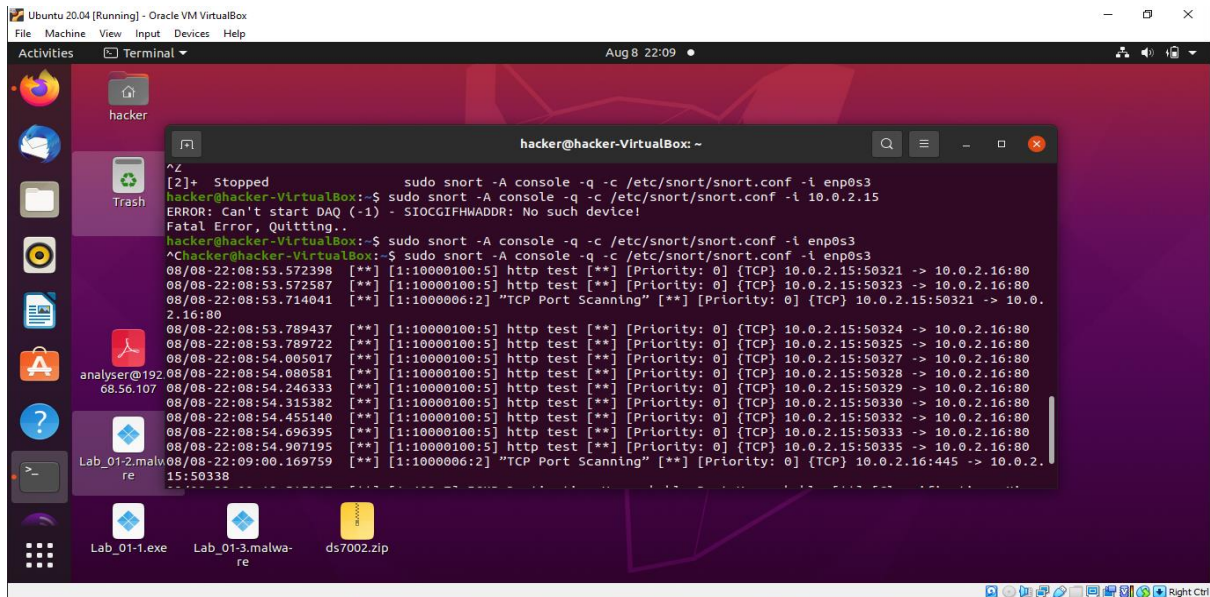


Figure. 27. NMAP scan



## Main Results

Snort detects TCP Port scanning below, 3<sup>rd</sup> line down after 'sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3' command is run which then triggers this alert.



```
hacker@hacker-VirtualBox: ~  
[2]+ Stopped sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3  
hacker@hacker-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i 10.0.2.15  
ERROR: Can't start DAQ (-1) - SIOCGIFHWADDR: No such device!  
Fatal Error, Quitting..  
hacker@hacker-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3  
^Z  
hacker@hacker-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3  
08/08-22:08:53.572398  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50321 -> 10.0.2.16:80  
08/08-22:08:53.572587  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50323 -> 10.0.2.16:80  
08/08-22:08:53.714041  [**] [1:1000006:2] "TCP Port Scanning" [**] [Priority: 0] {TCP} 10.0.2.15:50321 -> 10.0.  
2.16:80  
08/08-22:08:53.789437  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50324 -> 10.0.2.16:80  
08/08-22:08:53.789722  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50325 -> 10.0.2.16:80  
08/08-22:08:54.005017  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50327 -> 10.0.2.16:80  
analysier@192 08/08-22:08:54.080581  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50328 -> 10.0.2.16:80  
68.56.107 08/08-22:08:54.246333  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50329 -> 10.0.2.16:80  
08/08-22:08:54.315382  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50330 -> 10.0.2.16:80  
08/08-22:08:54.455140  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50332 -> 10.0.2.16:80  
08/08-22:08:54.696395  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50333 -> 10.0.2.16:80  
08/08-22:08:54.907195  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50335 -> 10.0.2.16:80  
Lab_01-2.malw 08/08-22:09:00.169759  [**] [1:1000006:2] "TCP Port Scanning" [**] [Priority: 0] {TCP} 10.0.2.16:445 -> 10.0.2.  
re 15:50338
```

Figure. 28. Snort Results from NMAP TCP Port scan

## IV. DESIGN SPECIFICATION

### A. Mitre Attack

For the lab and tools above this author researched a Cozy bear adversary campaign known as StellarParticle<sup>31</sup> which will be an example of a use case here for the design specification of this paper. According to CrowdStrike this campaign was related to the SUNSPOT implant from the SolarWinds intrusion in December 2020 and associated with Cozy bear(aka APT29, “The Dukes”). The aim of the author below is to show how adhering to the Mitre Attack framework that, that it’s possible to detect each stage of this specific attack with the use of tools used in the lab section of this paper.

Tactic	Technique	Observable	Detection
Credential Access	<b>T1003.006</b> OS Credential Dumping	Threat actor obtained credentials through domain replication protocols using Get-ADReplAccount command <u>DSInternal</u>	-Hayabusa scan as shown already in the above lab can detect <u>Mimikatz</u> as it has inbuilt rule to detect the <u>Mimikatz</u> tool used by <u>Cozy bear</u> and other Cyber threat groups.
Credential Access	<b>T1003.001</b> OS Credential Dumping: LSASS Memory	Threat actor used a heavily obfuscated Powershell script to execute the <u>Mimikatz</u> commands <u>'privilege::debug sekurlsa::logonpasswords "lsadump:: /patch"'</u> in-memory and encrypt the output	- <u>Again</u> a Hayabusa scan can detect <u>Mimikatz</u> as it has an inbuilt rule to detect <u>Mimikatz</u> tool used by <u>Cozy bear</u> and other Cyber threat groups. Early detection here would allow security personal to instigate mitigations early on to stop the attack vector.
Initial Access/Persistence	<b>T1078.003:</b> Valid Accounts: Local Accounts	A local account was used by the Threat Actor to establish a SSH tunnel into the internal network environment	-Snort can be used here to detect SSH tunnel - Sig 1-19559 is by default disabled and is used for SSH <u>BruteForce</u> detection. An alert rule can be added to <u>local.rules</u> file “ <u>alert tcp any any --&gt; any 22 (content:"SSH-2.0"; nocase; depth:7;)"</u> ”
Initial Access/Persistence	<b>T1133:</b> External Remote Services	The threat actor used VPNs to gain access to systems and persist in the environment	-Run a query from within Velociraptor to query windows event logs to look for Application log contents, logon session to detect unusual access patterns. Snort can be used to monitor network traffic flow to identify any unusual activity on the network.
Credential Access	<b>T1555.003:</b> Credentials from Password Stores: Credentials from Web Browsers	The threat actor exported saved passwords from user’s Chrome browser installations	- Hayabusa scan to monitor executed commands used to search for common password storage location to obtain user credentials, event logs in relation to file access to identify browser files that contain credentials

<sup>31</sup> “StellarParticle Campaign: Novel Tactics and Techniques | CrowdStrike,” crowdstrike.com, January 27, 2022, no. 31, <https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/>.

			such as Google Chrome's Login Data database  <u>file:AppData\Local\Google\Chrome\User Data\Default&gt;Login Data</u>
Credential Access	<b>T1539:</b> Steal Web Session Cookie	The threat actor stole web session cookies from end user workstations and used them to access cloud resources	- Snort can be used here to monitor for an attempt by a user to gain access to network or company resource <u>i.e.</u> cloud.  - Monitor for attempts by programs to inject into or dump browser process memory.
Lateral movement	<b>T1021.001:</b> Remote Services: Remote Desktop Protocol	The threat actor used both privileged and non-privileged accounts for RDP throughout the environment, depending on the target system	- Combination of Hayabusa and snort scans can be used to detect this here. Hayabusa to monitor for user accounts logged into systems associated with RDP  - Snort to monitor network traffic for uncommon dataflows that may use techniques to log into a computer using RDP.
Initial Access, Persistence	<b>T1078.004:</b> Valid Accounts: Cloud Accounts	The threat actor used accounts with Delegated Administrator rights to access other O365 tenants. The Threat actor also used valid accounts to create persistence within the environment.	-Velociraptor query to alert on event patterns of activity can be used to detect the use of valid and cloud accounts. If a hacker guesses the password for a valid <u>account</u> then the activity pattern is more like multiple failed logons followed by a successful logon on and might be easier to detect with this query in place.
Persistence	<b>T1546.003:</b> Event Triggered Execution: Windows Management Instrumentation Event Subscription	<u>TrailBlazer</u> was configured to execute after a reboot via a command-line event consumer	-Velociraptor has three specific queries in place here that could help in relation to WMI eventing visibility to help prevent this stage of an attack.  <u>Windows.Sysinternals.Autoruns</u>  <u>Windows.Persistence.PermanentWMIEvents</u>  <u>Windows.EventLogs.EvtxHunter</u>  ("WMI Event Consumers: what are you missing? :: Velociraptor - Digging deeper!," n.d.)

WMI Events<sup>32</sup> Velociraptor to help combat persistence above.

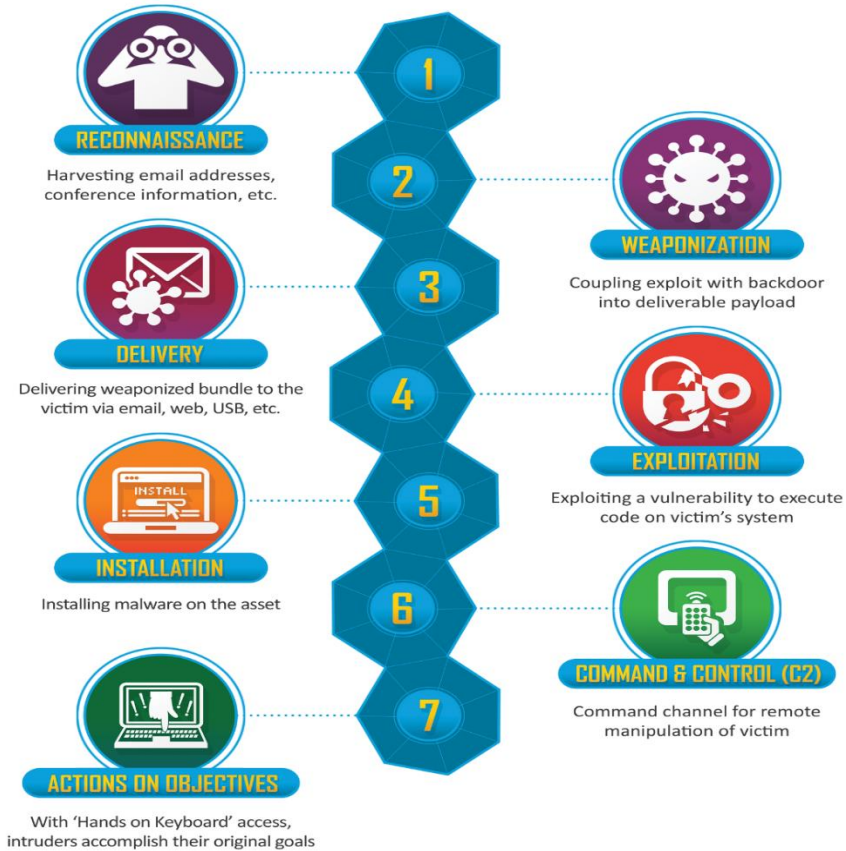
<sup>32</sup> "WMI Event Consumers: What Are You Missing? :: Velociraptor - Digging Deeper!," no. 32, accessed August 14, 2022, <https://docs.velociraptor.app/blog/2022/2022-01-12-wmi-eventing/>.

<p><u>Defense Evasion</u></p>	<p><b>T1036.005:</b> Masquerading: Match Legitimate Name or Location</p>	<p>The threat actor renamed their utilities to masquerade as legitimate system binaries (AdFind as svchost.exe), match the system's role (GoldMax), or appear legitimate (TrailBlazer as an apparent Adobe utility). Additionally, the threat actor renamed their systems prior to connecting to victim's VPNs to match the victim's system naming convention</p>	<p>-File <u>MetaData</u> – Collect file hashes, files not matching their expected hash are suspicious. <u>Velociraptor</u> artifact <u>Generic.Forensic.LocalHashes.Glob</u> – maintains a local database of file hashes. You can query this database using the <u>Generic.Forensic.LocalHashes.Query</u> artifact</p>
-------------------------------	--	---	--

**V. IMPLEMENTATION**

The implementation stage of this paper will aim to show how mitigations at each stage of the Cyber Kill Chain framework can help to kill an attack from Cozy bear and other hacking groups.

**A. Cyber Kill chain**



**Figure. 29.** Cyber Kill chain

#### a) **Reconnaissance – Stage 1**

The attacker attempts to gather as much information about the target prior to an attack. This could be anything from researching an organisation on the web, phone calls or emails to employees or dumpster diving. Port scanning of organisation endpoints is an example of another information gathering technique, used here.

##### **Defences:**

- Employee cyber awareness, social engineering campaigns including spam email, what to look out for.
- Evaluate company assets, is there a need for access to certain services, confidential data available on public-facing assets (websites etc..). Make social media accounts private.
- Snort - **Snort network recon techniques**<sup>33</sup> to detect port scanning by alerting on an unusual number of connection requests within a short period of time you can use Snort's detection filter rule below.

```
"alert tcp any any -> $HOME_NET any (msg:"TCP Port Scanning"; detection_filter:track by_src, count 30, seconds 60; sid:1000006; rev:2;)"
```

By adding the command at the bottom of the local.rules snort file it will limit the alerts with the sid of 1000006 to 1 per every 60 seconds, this is important in relation to a scan of a large network.

```
event_filter gen_id 1, sig_id 1000006, type limit, track by_src, count 1, seconds 60
```

##### **Results:**

As displayed earlier in this paper Snort picks up on the Nmap TCP Port scanning activity see last line on the grab below. While any endpoint connected to the internet will be subject to continuous port scanning, there are several mitigations that security professionals can put in place, with the installation of a firewall being one. A firewall can detect a port scan and slow it and effectively shut them down.

There are other ways to defend against Nmap scanning, such as:

- Hiding services on obscured ports
- Running own scans to detect vulnerabilities and fixing
- Port knocking
- Honeypots and honey nets
- OS Spoofing

---

<sup>33</sup> "Snort Network Recon Techniques," Infosec Resources, no. 33, accessed August 14, 2022, <https://resources.infosecinstitute.com/topic/snort-network-recon-techniques/>.



```

hacker@hacker-VirtualBox: ~
^Z
[2]+ Stopped sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
hacker@hacker-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i 10.0.2.15
ERROR: Can't start DAQ (-1) - SIOCGIFHWADDR: No such device!
Fatal Error, Quitting..
hacker@hacker-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
^Chacker@hacker-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
08/08-22:08:53.572398  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50321 -> 10.0.2.16:80
08/08-22:08:53.572587  [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50323 -> 10.0.2.16:80
08/08-22:08:53.714041  [**] [1:1000006:2] "TCP Port Scanning" [**] [Priority: 0] {TCP} 10.0.2.15:50321 -> 10.0.2.16:80

```

Figure. 30. TCP Port Scanning alert

**b) Weaponization – Stage 2**

This stage involves the bad guys preparing malware to deliver to an organisation, which can be developed on results from the reconnaissance stage.

**Defences:**

By understanding vulnerabilities and preparing personal in an organisation, companies have the chance to weaken or eliminate a threat actors’ ability to weaponize data they collect about their environments.

- Regular Vulnerability scans to detect scripting errors on websites for example
- Annual penetration tests
- Patching all resources and keeping up to date
- Cyber awareness of all employees. Sending fake phishing emails all to lessen sisk of social engineering attacks.

**c) Delivery - Stage 3**

Delivery stage is where the attacker will attempt to deliver a malicious payload to an organisation, with spear phishing email attacks one of the preferred methods used by the Cozy bear threat group.

**Defences:**

- User education on top of proper security controls is paramount
- Microsoft Group policy to disable email hyperlinks
- Add Snort rules to alert IT admins of blocked attempts of access for example brute force attack.

Below is a Snort rule to detect a Hydra attack:

```

alert tcp $SMTP_SERVERS 465 -> $EXTERNAL_NET any (msg:"SMTP AUTH LOGON brute force attempt"; flow:from server,established; detection filter:track by dst, count 5, seconds 60; metadata: service smtp; classtype:suspicious-login; sid:2278; rev:2;)

```

**d) Exploitation – Stage 4**

This stage involves a targeted user clicking on a malicious file or link in a spam email to unleash malware or direct the victim to bogus url links.

**Defences:**

- Anti-Malware installed in an environment will help block infected attachments.

- Web proxy filtering to block access to bogus/malicious websites.

**e) Installation – Stage 5**

At this stage an infected file such as malware is downloaded onto the targeted users machine.

**Defences:**

- Its important users do not have local admin rights on devices to mitigate and prevent installation of malware on a local networked machine.

**f) Command & Control (C2) – Stage 6**

This stage is where the hacker/s now have control of a user's device. From here they can access an organizations network further, moving laterally and looking for other targets such as sensitive data and admin accounts to exploit or elevate privileges.

- Endpoint protection software can help detect if a suspicious link has been clicked by a member of the organization
- Web proxy can help here to detect if malware has been downloaded onto a company machine
- User and entity behavior analytics (UEBA)<sup>34</sup> is a cybersecurity solution that can be used to help detect anomalies in the behavior of not just users on a network but also devices connected to it such end points, routers and servers to alert network defenders if a hacker is lurking on their network.

**g) Actions on Objectives – Stage 7**

At this stage the bad actor has reached their primary goal to steal data and move it external to the network they stole it from or unleash malware to lock down an organization's files.

**Defences:**

- DLP software could be used here to prevent data been moved external to the network that has been breached.
- Web proxy control to prevent removal of files
- Block access to website that could be used to transfer data, [www.wetransfer.com](http://www.wetransfer.com) is an example of one such site.

**B. ISO27001 – Monitoring and Measurement**

The final part here is how to tie all this back into the continuous monitoring and measurement according to clause 9.1 of ISO27001 security framework, by way of implementation. This clause compares information security performance v ISMS effectiveness. Availability of information, response time to an event and the costs involved to protect data all have to be weighed up here.

- What needs to be monitored and measured against
- Tools or methods to be used for monitoring and measurement
- When monitoring and measurement needs to be done

---

<sup>34</sup> "What is UEBA? Definition and use," FireEye, no. 34, accessed August 14, 2022, <https://www.fireeye.fr/products/helix/what-is-ueba.html>.

- Results to be analysed and evaluated
- Who carries this out

Securing networks and data needs to be the number one goal of any organisation. Although, there must be a balance in relation to costs of security v ISMS effectiveness. It is worth noting the security tools and frameworks researched in this paper are all free to use, so costs can be kept to a minimal when implementing these tools and frameworks into any size organisation. With the main costs attributed to the installation, configuration, testing, maintenance, and monitoring by security professionals whether in-house or vendor related. Satisfying this clause should be achievable for all organisations using the tools researched and adhering to frameworks as highlighted in this paper.

**Open-Source tools:** Hayabusa, Snort, Velociraptor, Pestudio

**Free to follow frameworks:** Mitre Attack, Cyber Kill chain, ISO27001(if certification required then need to pay for this)

## VI. CONCLUSIONS

In this paper, the author performed an analysis of the Cyber hacking group known as Cozy bear, APT29. Focusing on understanding its attack profile and how to actively defend against its malicious intent. The author argued throughout this work that the use of threat hunting tools such as Velociraptor, Hayabusa and PeStudio and security frameworks such as mitre attack, kill chain and ISO27001 can help defend against the Cozy bear group. This paper challenged the conventional ideas about how to protect a network from attack with use of previously well-known frameworks to relatively newly developed security tools. Yet the fight against these threat actors as they evolve and change their attack methods should not be underestimated.

Next steps, this paper and tools researched combined could be used in future malware campaigns to protect against the people behind Cozy bear. As has been seen in recent years, this malicious hacking group have evolved their techniques and targets so that no organization is safe from their clutches. But with the research seen in this paper and with further study in this field it is possible to protect against the Cozy bear hacking group.

**Video Presentation link:** <https://youtu.be/Xgh6xu97sq0>



## VII. REFERENCES

- Abe, Hiroshi, Keiichi Shima, Yuji Sekiya, Daisuke Miyamoto, Tomohiro Ishihara, and Kazuya Okada. "Hayabusa: Simple and Fast Full-Text Search Engine for Massive System Log Data." In *Proceedings of the 12th International Conference on Future Internet Technologies*, 1–7. CFI'17. New York, NY, USA: Association for Computing Machinery, 2017. <https://doi.org/10.1145/3095786.3095788>.
- "About Hayabusa." Rust. 2020. Reprint, Yamato Security 大和セキュリティ, August 14, 2022. <https://github.com/Yamato-Security/hayabusa>.
- CrowdStrike Adversary Universe. "Adversary: Cozy Bear - Threat Actor." Accessed August 14, 2022. <https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/>.
- "Advisory: APT29 Targets COVID-19 Vaccine Development." Accessed August 14, 2022. <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development>.
- "Advisory Further TTPs Associated with SVR Cyber Actors.Pdf." Accessed August 14, 2022. <https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf>.
- Aickelin, Uwe, Jamie Twycross, and Thomas Hesketh-Roberts. "Rule Generalisation in Intrusion Detection Systems Using SNORT." *International Journal of Electronic Security and Digital Forensics* 1, no. 1 (January 2007): 101–16. <https://doi.org/10.1504/IJESDF.2007.013596>.
- SOCRadar® Cyber Intelligence Inc. "APT Profile: Cozy Bear / APT29," November 16, 2021. <https://socradar.io/apt-profile-cozy-bear-apt29/>.
- "Artifacts :: Velociraptor - Digging Deeper!" Accessed August 14, 2022. <https://docs.velociraptor.app/docs/gui/artifacts/>.
- "Chapter 11. Defenses Against Nmap | Nmap Network Scanning." Accessed August 14, 2022. <https://nmap.org/book/defenses.html>.
- cr00t. "Install Velociraptor Client on Linux and Windows Systems - Kifarunix.Com," January 8, 2021. <https://kifarunix.com/install-velociraptor-client-on-linux-and-windows-systems/>.
- Lockheed Martin. "Cyber Kill Chain@," June 29, 2022. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.
- "Cyber Security Threat Modeling Based on the MITRE Enterprise ATT&CK Matrix | SpringerLink." Accessed August 14, 2022. <https://link.springer.com/article/10.1007/s10270-021-00898-7>.
- ISO. "ISO - ISO/IEC 27001 — Information Security Management." Accessed August 14, 2022. <https://www.iso.org/isoiec-27001-information-security.html>.
- "Main Directorates of the Armed Forces General Staff." Accessed August 14, 2022. <https://www.globalsecurity.org/military/world/russia/mo-general-staff-1.htm>.
- ICT Institute. "Measuring and Monitoring Your ISO 27001 ISMS," March 10, 2022. <https://ictinstitute.nl/measuring-and-monitoring-your-iso-27001-isms/>.
- Neo4j Graph Data Platform. "Neo4j Desktop - Neo4j Browser." Accessed August 14, 2022. <https://neo4j.com/docs/browser-manual/4.4/deployment-modes/neo4j-desktop/>.
- "Rekall Discontinuation." Python. 2014. Reprint, Google, August 3, 2022. <https://github.com/google/rekall>.
- "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA." Accessed August 14, 2022. <https://www.cisa.gov/uscert/ncas/alerts/aa22-110a>.
- "Rust Programming Language." Accessed August 14, 2022. <https://www.rust-lang.org/>.
- "Snort - Network Intrusion Detection & Prevention System." Accessed August 14, 2022. <https://www.snort.org/>.
- Infosec Resources. "Snort Network Recon Techniques." Accessed August 14, 2022. <https://resources.infosecinstitute.com/topic/snort-network-recon-techniques/>.
- son, do. "Hayabusa v1.4.3 Releases: Windows Event Log Fast Forensics Timeline Generator and Threat Hunting Tool." Penetration Testing, December 31, 2021. <https://securityonline.info/hayabusa-windows-event-log-fast-forensics-timeline-generator/>.
- crowdstrike.com. "StellarParticle Campaign: Novel Tactics and Techniques | CrowdStrike," January 27, 2022. <https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/>.
- Team, Threat Hunter. "Attacks Against the Government Sector (White Paper)," n.d., 21.

Rapid7. "Understanding and Configuring Snort Rules | Rapid7 Blog," December 9, 2016.  
<https://www.rapid7.com/blog/post/2016/12/09/understanding-and-configuring-snort-rules/>.

User, Import. "Introducing Osquery." *Engineering at Meta* (blog), October 29, 2014.  
<https://engineering.fb.com/2014/10/29/security/introducing-osquery/>.

"Welcome :: Velociraptor - Digging Deeper!" Accessed August 14, 2022.  
<https://docs.velociraptor.app/>.

"What Is GRR? — GRR Documentation." Accessed August 14, 2022. <https://grr-doc.readthedocs.io/en/v3.2.1/what-is-grr.html>.

"What Is the MITRE ATT&CK Framework? - Palo Alto Networks." Accessed August 14, 2022.  
<https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-framework>.

FireEye. "What is UEBA? Definition and use." Accessed August 14, 2022.  
<https://www.fireeye.fr/products/helix/what-is-ueba.html>.

"WMI Event Consumers: What Are You Missing? :: Velociraptor - Digging Deeper!" Accessed August 14, 2022. <https://docs.velociraptor.app/blog/2022/2022-01-12-wmi-eventing/>.

"YARA: Effective Tool to Detect Malware." Accessed August 14, 2022.  
<https://www.cyber.nj.gov/informational-report/yara-effective-tool-to-detect-malware>.

Zorz, Mirko. "Pestudio: Initial Malware Assessment Made Simple." *Help Net Security* (blog), June 16, 2016. <https://www.helpnetsecurity.com/2016/06/16/pestudio-initial-malware-assessment/>.