CYBER MONGOL

COUNTER CYBER INTELLIGENCE

1.15.22

CONTENTS

THE NEED

Initially, Cyber Mongol was founded as a systems integrator, specifically focusing on cloud integration, security and compliance. Working with the sophisticated defensive technologies of the day, we shortly came to realize that there was a vast cavern between the capabilities of adversaries and those tasked to stop them. There was an ever-expanding skills gap which didn't favor the blue side, partially amplified by the industry's push for certification over practical skill, fueled further by unrealistic expectations of hiring managers – or unicorn hunters. The panacea of machine learning wasn't what (or still isn't) what it promised, leaving those working with these defensive technologies feeling uneasy and outgunned.

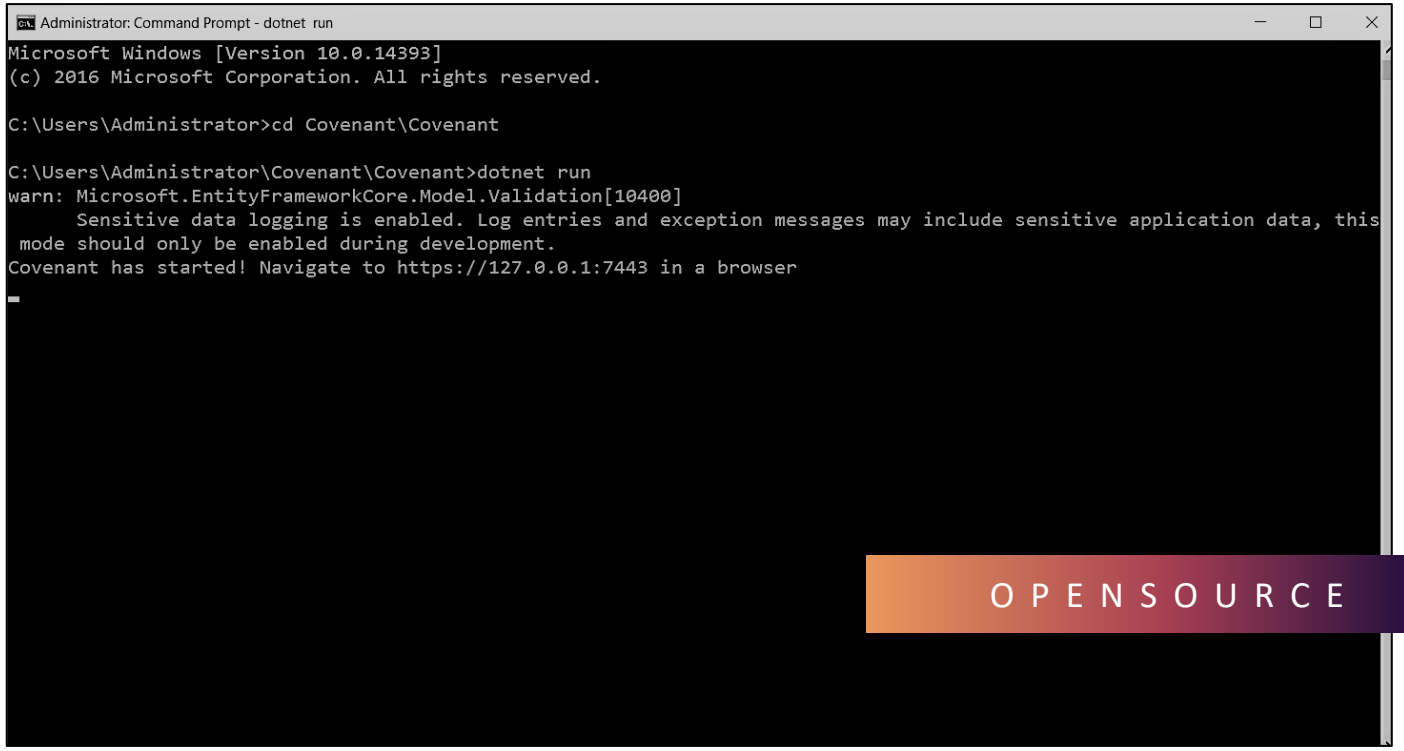
In contrast to this, there was (is) a niche of security experts working for the blue side, extremely skilled and producing content that pushes the ecosystem forward as a whole. Consuming this awesome resource (output from the top skilled one percent within the cybersecurity ecosystem) for defensive purposes was not without its own set of challenges, but we understood that we better get good at it because adversaries are proficient consumers of this opensource resource. The first challenge in consuming this resource is the skills barrier-to-entry. Simply put, this niche social structure within the cybersecurity ecosystem is of advanced skill-level and that is the skill-level needed to access this knowledge base. The second of these challenges was to know where to look and when to look for it. This resulted in our team continually reading content across social platforms and repeatedly triaging data manually. The nature of this time-consuming and arduous task motivated what would be the core of Cyber Mongol's technology, automation that ingests, triages, classifies, correlates social and software structures, and articulates human momentum and offensive behaviors from within the cyber security ecosystem. We knew that if we could "team up" with advanced automation to anticipate innovation / trends in offensive operator tactics, we would have a chance of at least keeping pace with the adversaries who use them.

While traditional cyber intelligence capabilities play an important role in the defense strategy of an organization, our team knew we needed a deeper understanding of how adversaries may or are currently, penetrating IT systems. It's no secret to the defensive community that advanced adversaries keenly observe the top one percent of the cybersecurity ecosystem and the advancements in opensource tool systems they produce. From an adversary's perspective, these exploit tool systems offer some significant advantages over in-house developed solutions.

As offensive operators push for greater operational security, opensource or commoditized tooling will enhance anonymity and obscure attribution efforts. Moreover, just like any other enterprise, controlling innovation costs (whether measured in time or literal dollars) can greatly increase the number of campaigns an adversary is able to wage, when leveraging already existent innovation from the top one percent of the cyber security ecosystem.

In a recent report [3], Recorded Future published that over 40 percent of their detections in 2020 for adversary tools (Command & Control and Remote Access Trojans) were opensource based.

Below, we will explore the tightly coupled system of elite cybersecurity content generators, advanced adversaries and the bi-directional influence both groups exhibit over each other. Much like observing leading economic indicators in the stock market may signal movement within the broader market, Cyber Mongol uses its technology to look for movements within the cybersecurity ecosystem to anticipate advanced operator tradecraft adoption.



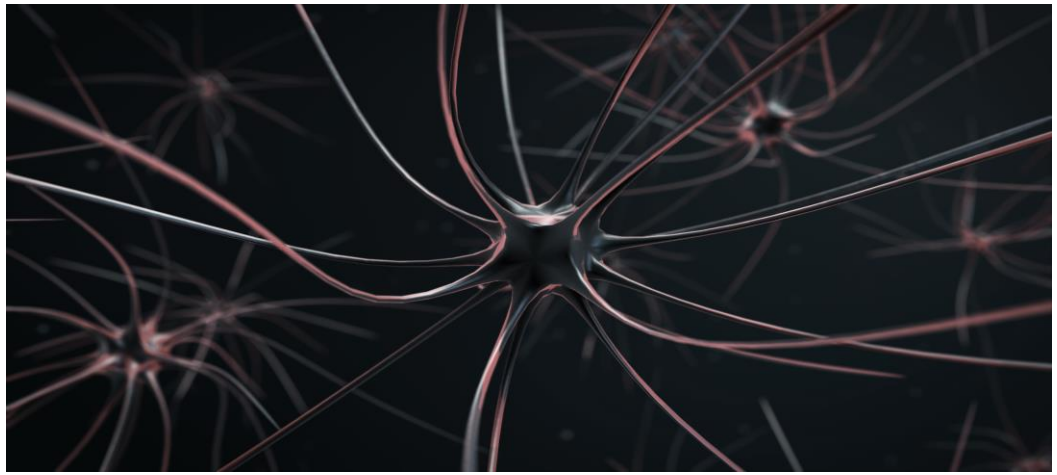
It is important to understand how these two groups (cybersecurity elite / advanced adversaries) influence each other's output, to understand how we may collect counter cyber intelligence (CCI). Let's look at two different scenarios where the influence is reversed and how effective CCI may be distilled.

In scenario one, a nation-state has purchased a zeroday from an underground broker in utter secrecy and begins to fulfill their intended objectives. During their attack, the adversary is detected by defenders and threat intelligence is shared with the broader security community. Utilizing the shared threat intelligence on the recent attack and possibly reverse engineering a recent mitigation patch, the elite members within the cybersecurity ecosystem are able to engineer a working proof-of-concept for the zeroday and disseminate it publicly. This in turn spurs further adoption by those adversaries watching the security ecosystem for innovation. It is before that event (mass adversary adoption) and right after the first release of publicly available exploit code, that the opportunity for counter cyber intelligence exists. A similar scenario is currently playing out with HAFNIUM's recent exploit chain which was caught targeting Exchange Servers [4] and now has code circulating within the cybersecurity ecosystem.

In scenario two, elite members of the cybersecurity ecosystem produce an effective way to circumvent current defensive technologies. This tradecraft is then articulated and disseminated down their social channels, observed and then adopted by advanced adversaries.

This is the point where counter cyber intelligence can be extremely effective, anticipating adversary tradecraft adoption before an active campaign takes place. More will be said regarding this aspect of prediction as it incorporates specific Cyber Mongol methodologies for analyzing social structures involved with articulation and dissemination of tradecraft.

This scenario is also occurring within the same HAFNIUM campaign, with HAFNIUM's use of procdump.exe to dump lsass.exe. Back in late summer of 2019, our automation was ingesting large volumes of tradecraft associated with exactly this vector. This vector was also employed effectively by Iranian operators and articulated in a threat report dubbed FoxKitten [5], February 2020. Lastly, it is important to mention that effective CCI shouldn't necessarily look for new tradecraft, rather it should look for new human momentum behind old or new tactics.

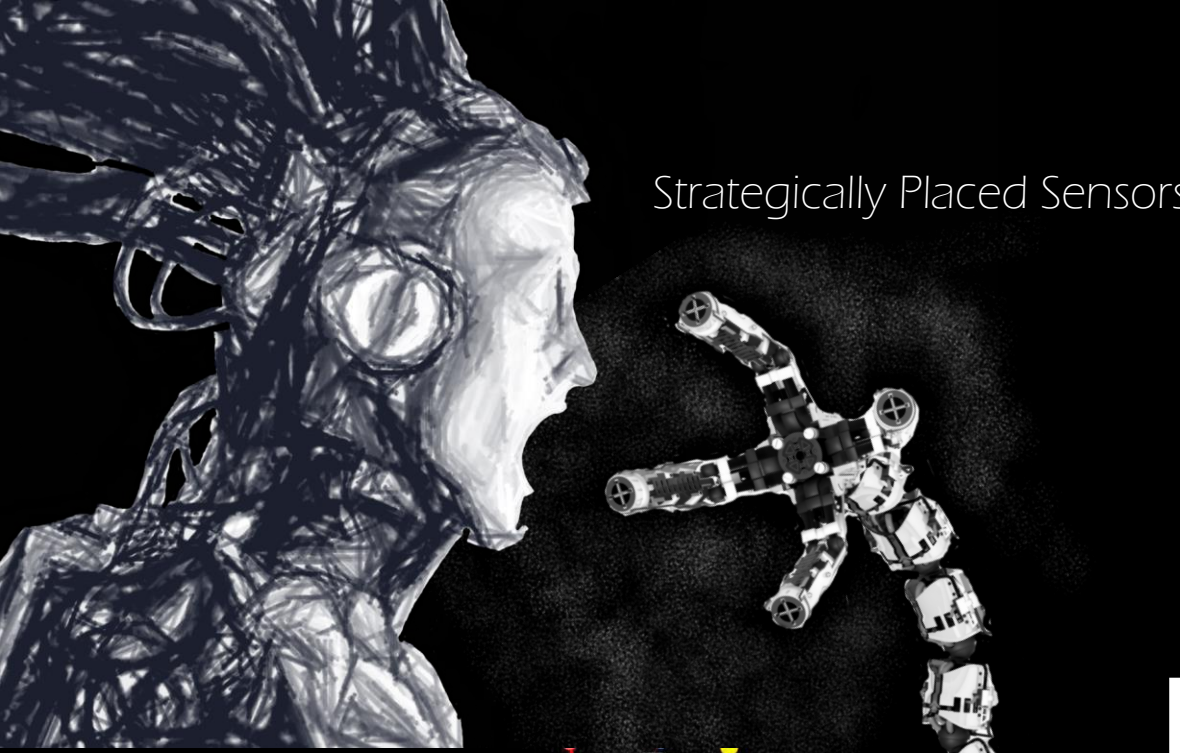


PANDEMIC

COUNTER CYBER INTELLIGENCE

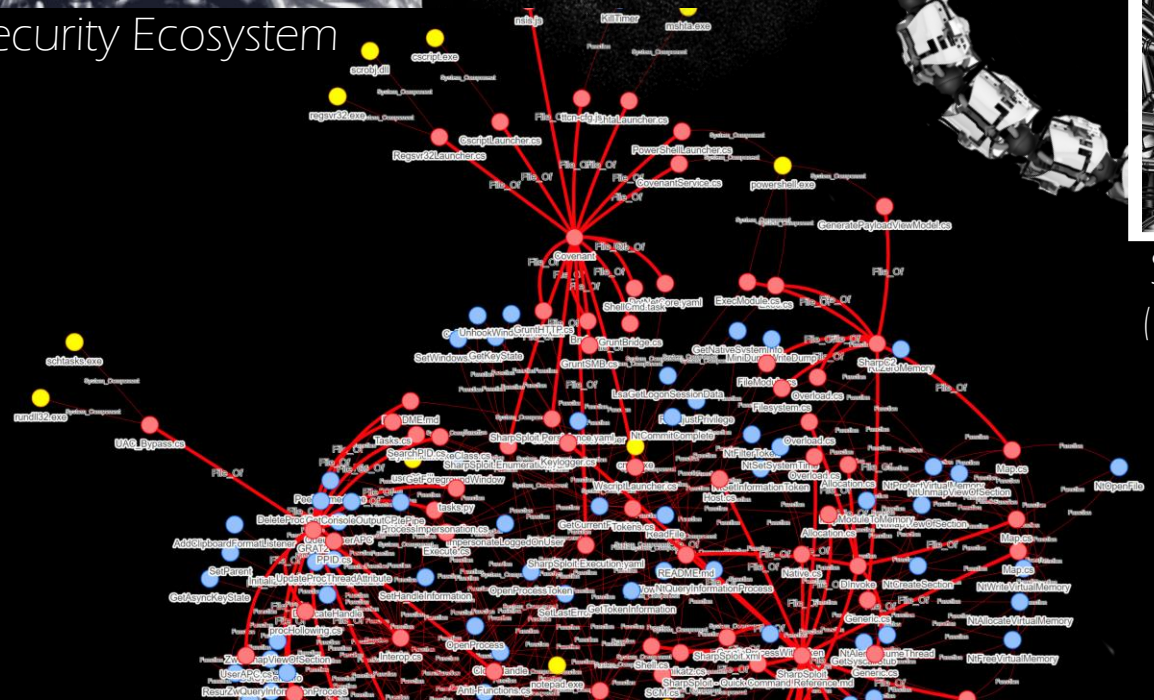
BACKEND AUTOMATION

PANDEMIC Counter Cyber Intelligence Automation is a modular pipeline built to automate the laborious task of opensource intelligence collection as it relates to the identification of advanced operator tactics.

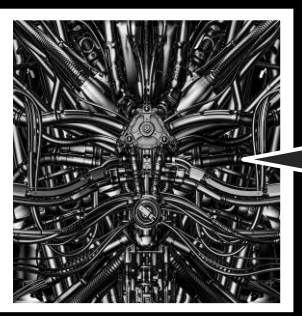


Strategically Placed Sensors

Security Ecosystem



Backend Automation Components



Sensor Triage
(Chatter, Content, Code Creation)

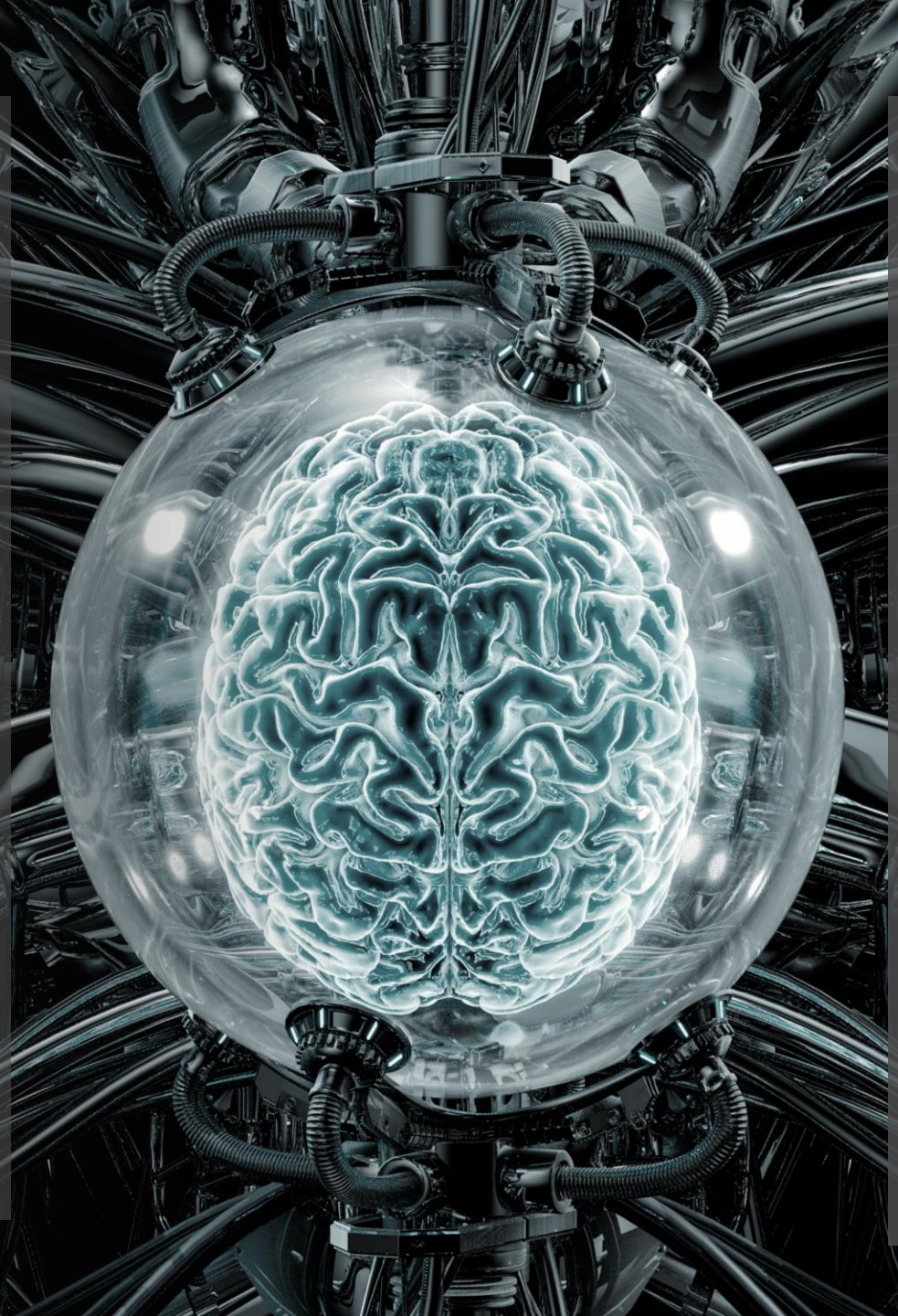
Live Analysis
(Pillars, Trends, New Signals)

Relationships
Social, Software, Behavior

Automated Threat Analysis

Visualize Data
Exploit & Exploit Tool Relationships, Social Relationships, Source code Relationships, Behaviors

Curated Data



Pipeline Ingress
At the ingress of the pipeline are strategically placed sensors with the sole purpose of observing human activity within the cybersecurity ecosystem and distilling signals.

Triage
These signals are then triaged by the automation as to weed out unnecessary or irrelevant data which are not aligned with the automation's objectives.

Live Analysis
It is at this point that the automation visualizes the first bit of usable insight. Human momentum (and signal pillars discussed later) behind various exploits and exploit tool systems can be quantified and compared, in relation to each other.

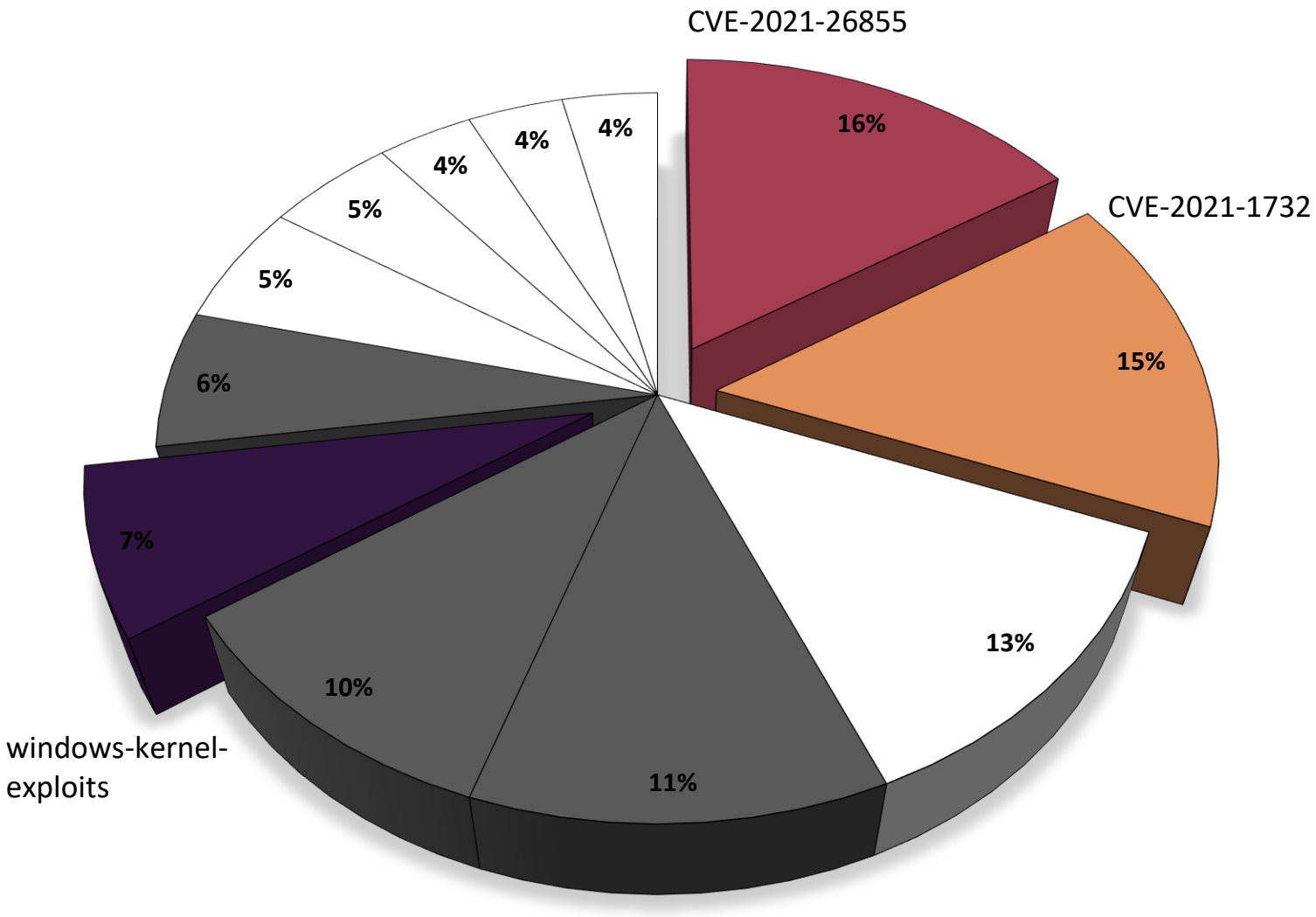
Relationships
Detailed graphs are built consisting of social structures, software relationships and tradecraft behavior similarities.

Distillation
At this point, the automation creates specific tradecraft profiles that consist of text processing features, API calls, Windows native system binaries and associated privileges found within the ingested tradecraft.

Thoth Module
Thoth’s primary purpose is to identify tradecraft which targets Windows platforms, dismantle the source code by Windows functions and parameters and then build graph structures representative of that source code. Lastly, Thoth looks to group these code snippets by MITRE defined behavior types for consumption by ASATA.

Pipeline Egress
The automation’s output is highly curated threat signals representative of adversary tradecraft that is currently trending or may be soon adopted. Additionally, PANDEMIC produces highly detailed social structures depicting relationships within the cybersecurity ecosystem.

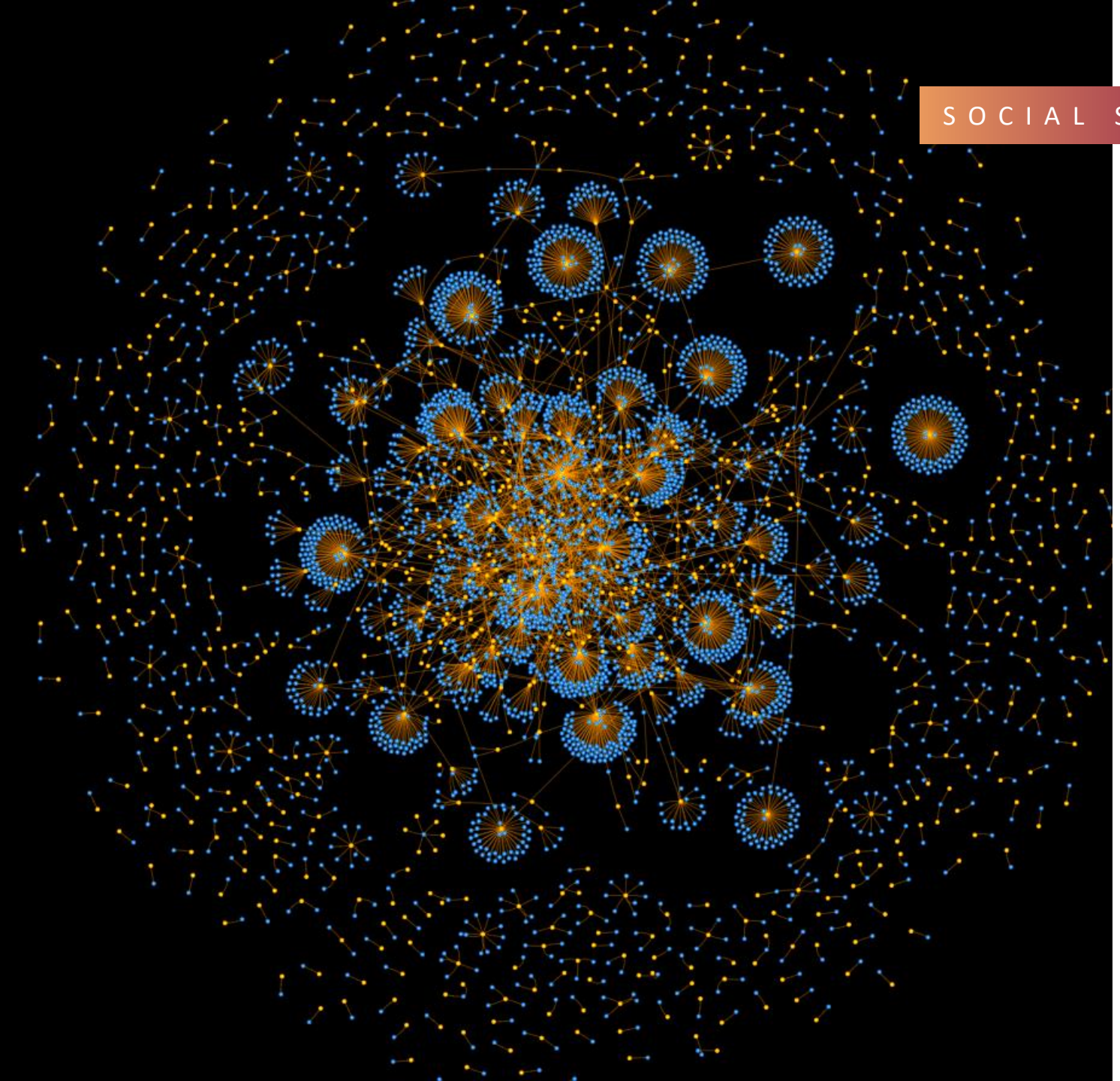
HUMAN MOMENTUM



Registering and analyzing human momentum within the cybersecurity ecosystem is a very effective way to gauge on-trend activity. Moreover, analyzing human momentum has a triaging effect on its own, visualizing only what is gaining momentum based on what others within the ecosystem deem important.

There are two distinct classes of momentum that we register and analyze – pillar signals and those signals that approach, equal or surpass them. We define pillar signals as signals which consistently show predictable human momentum, day-in, day-out. Contrasting emerging signals with pillar signals is a great way to assess the overall velocity or human excitement of an emerging signal. Should an emerging signal surpass a pillar signal which typically registers large momentum volume, it is safe to say that that signal is generating quite a buzz within the cybersecurity ecosystem.

The pie chart on the left depicts human momentum over a 12-hour period (truncated). The pillar signals are greyed out (Routersploit (11%), PoC-in-GitHub (10%), Metasploit (6%)) and signals of interest are coloured. We can see that the first two signals (CVE-2021-26855 (16%), CVE-2021-1732 (15%)) have blown passed all pillar signals and for good reason, they both represent exploit code recently utilized in advanced adversary campaigns which have become publicly available [4] [6]. This is an early warning sign that further adversary adoption and mass exploitation may be imminent.

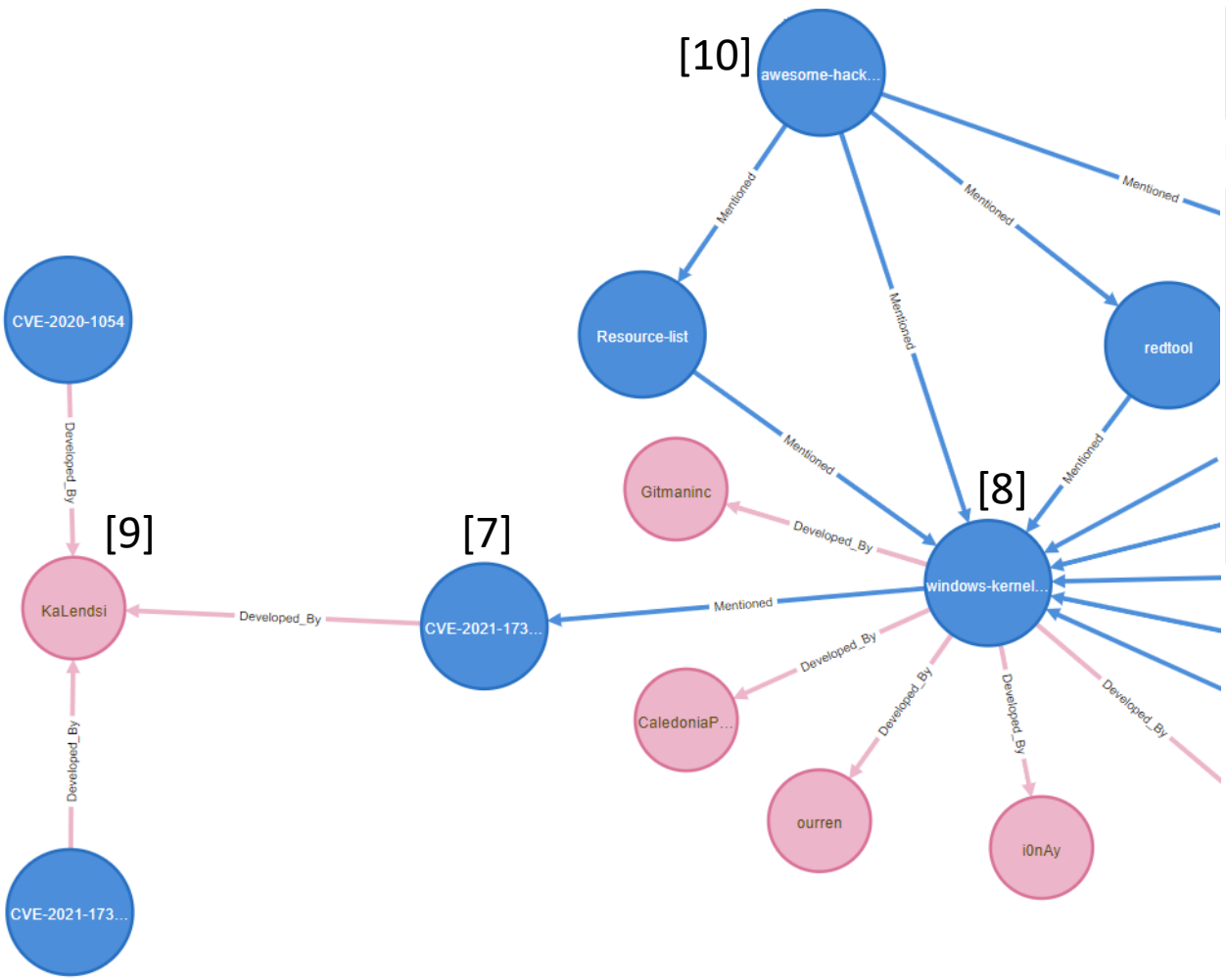


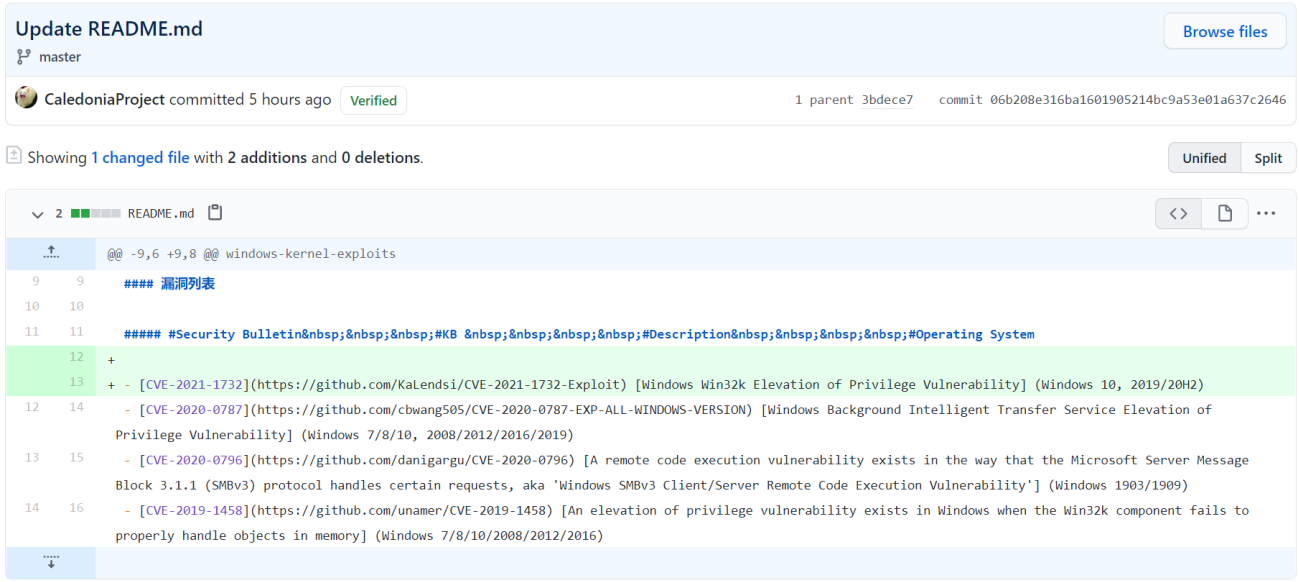
SOCIAL STRUCTURES

Just as within a society, social structures exist within the cybersecurity ecosystem and can be used to greatly enrich counter cyber intelligence efforts. The nature of graph databases lends itself extremely well to the storing and analysis of these social structures, making graphs an important component within a CCI automation stack. The examination of connections within these social structures can reveal powerful amplification channels, tradecraft efficacy predictors and visualize migrations in already existent tradecraft. When the context of social structures is paired with human momentum indicators, a forward-looking and unique threat landscape is depicted, empowering CCI objectives.

Our CCI automation maps two very specific relationships as it relates to social structures:

Content that is -[Developed_BY]-> an author and content that -[Mentions]-> other content.





Drilling down on tradecraft exemplified in the human momentum pie chart, we can look at the related social structure (simplified) for CVE-2021-1732 [7], a Win32.sys Elevation of Privilege Vulnerability. To the right, there is a "Mentioned" relationship with windows-kernel-exploits [8] and to the left, a "Developed_by" relationship with KaLendsi [9]. Out of these two relationships, the relationship with windows-kernel-exploits is most meaningful as it acts as a social amplification channel for CVE-2021-1732.

This amplification happens because of the large social reach or the social attraction windows-kernel-exploits has over the cybersecurity ecosystem as a whole. The greater the amplification effect, the greater the chance an adversary will see it and ultimately adopt the exploitation tactic. This amplification channel would have definitely contributed to the overall human momentum seen for CVE-2021-1732, in the previous pie chart.

If we follow the social structure further, we see that windows-kernel-exploits is itself being amplified by another tradecraft aggregation, awesome-hacking-lists [10], further compounding the amplification effect.

An interesting observation is that these repos [7] [8] [9] [10] all belong to the Chinese security community, precisely where the first victim reports emerged [6] of CVE-2021-1732 being exploited in the wild.

Considering the human momentum behind CVE-2021-1732 and its double amplified social structure, this could indicate that there is much greater potential for widespread adversary adoption for this Elevation of Privilege Vulnerability.

ASATA

Advanced Skills & Adversary Tactics Articulation

CYBER MONGOL

OPERATIONALIZE

Search across 1 million Windows functions used in today's most popular offensive tradecraft. Operators can filter their search criteria by Windows functions, function parameters and MITRE defined behavior types. ASATA observes real-time trends in the cybersecurity ecosystem so as to continually grow the offensive codebase made available to search.

Get a rapid understanding of how adversaries build their tactics by seeing a visual layout of the codebase. Further tactic comprehension is bolstered by being able to select MITRE defined behavior types and having the corresponding source code visualized. Interface users are able to click on called functions and their parameters to get the related MSDN documentation and jump directly into the source code to where those functions and parameters are used.

ASATA is built atop advanced cyber intelligence automation that continually monitors the cyber security ecosystem. Human activities within that ecosystem are measured and mapped, allowing ASATA to alert its users to new and emerging trends in exploitation.