CYBER INTEL MATRIX

White Paper Case Study

The COVID-19 Pandemic Effect on Cybercrime

WHAT IS THE CYBER INTEL MATRIX (*CIM*) HONEYPOT SYSTEM?

Our global honeypot system, called the CIM BlackPot system, is the largest Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) control system architecture honeypot system in the world.

Such an enormous, complex world of a system is necessary for creating an effective Cyber Threat Intelligence (CTI) platform because there is still little information about SCADA vulnerabilities and attacks, despite the growing awareness of security issues in industrial networks. Because of the nature of IT security, owner-operators are often unwilling to release attack or incident data. Although some vulnerability research is being conducted in this area, very little has been released publicly, and no "SCADA security tools" (whatever that might mean) have been released to the public. By providing a range of common industrial control protocols, we have created the basics for building your own system that is capable of emulating complex infrastructures.

The infrastructure convinces adversaries that they just found and infiltrated a huge industrial complex. This is essential, because otherwise honeypots look like honey, and even moderately sophisticated hackers will turn away, or otherwise game the system, and there will be no ability to study behavioral patterns, strategies, accomplices, or specific intentions.

To improve the deceptive capabilities of our BlackPot system, we also provided a custom human-machine interface, in order to increase the honeypot attack surface. The response time of the services also can be artificially delayed, to mimic the behavior of a system under constant load.

COVID-19 ***CIM* BlackPot™ / CTI** CASE STUDY:

SUMMARY:

The COVID-19 pandemic not only poses a threat to our health, but also to our businesses and governments. Our data gathering and analyses show that cybercriminal activity has risen consistently in step with outbreak peaks in regions around the world. The correlation suggests that as citizens, corporate entities, and governments focus on saving lives, cybercriminals use the diversion to penetrate systems worldwide.

This case study report analyzes the criminal activity three months after the official COVID-19 outbreak in Wuhan, China—mid-December 2019 through mid-March 2020. The damaging impact on the online IT infrastructure, and on the existing measures in place to protect individuals, organizations, and countries, is significant.

Herein we demonstrate the findings and our *CIM*-CTI analysis, based on social media platforms, the Dark Web, and attacks to our global BlackPot system, where we engaged hackers so that we could observe, capture, and analyze their behavior, keywords, and patterns. This engagement creates an ongoing intel database on-the-fly.

THE FINDINGS:

Incidents affecting individuals

1. Social engineering crimes leveraging COVID-19. Fear is the easiest emotion to abuse for malicious purposes, and the foundation of a well-designed social engineering campaign. Because the fear over COVID-19 is rampant, pretty much every

method cybercriminals have tucked into their toolbox is working, making these the most rampant types of incident:

- ► Fake news distribution
- ► Spamming
- ► Phishing campaigns
- ► Malspam campaigns
- ► Installing malware

The goals of these incidents: stealing money, collecting information for future attacks, phishing, and distributing related malicious programs.

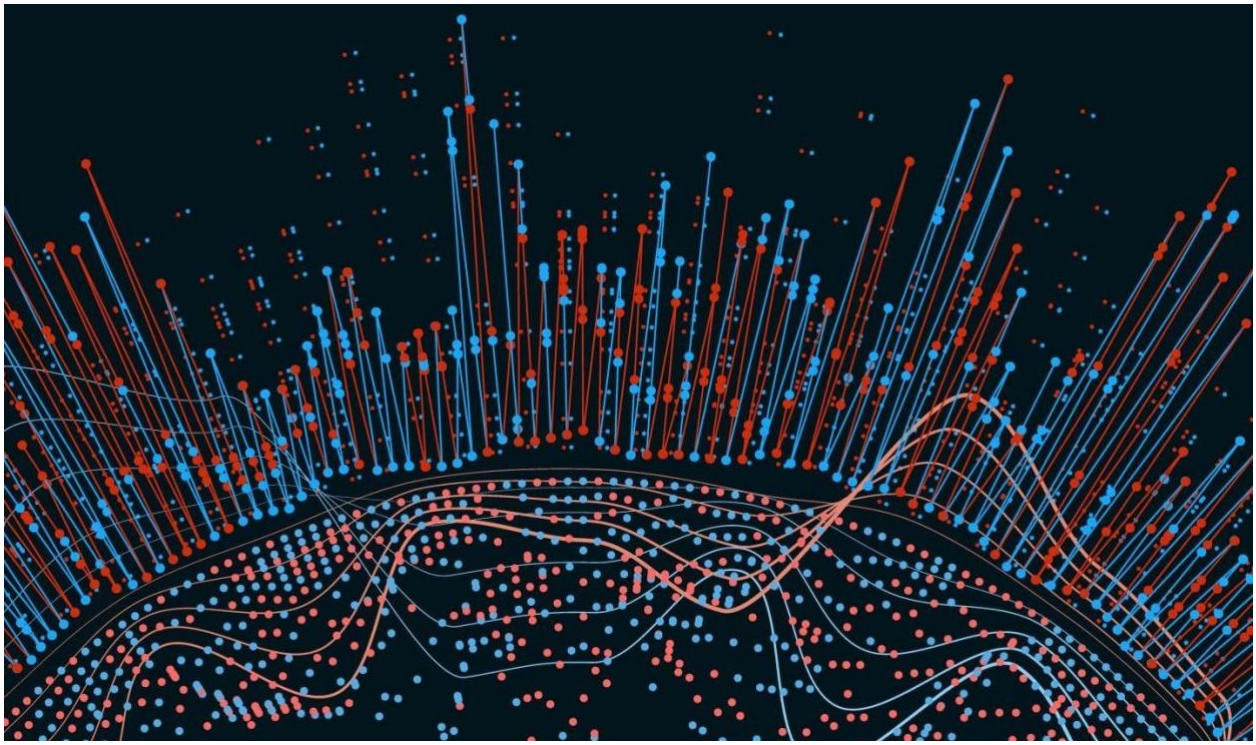
Typical new scams include persuading people to do the following: donate money for a children's vaccine, when neither the vaccine, nor the charity organization, exist; purchase products like face masks and toilet paper. The moment people click the pay button, the order amount is stolen, along with sensitive personal and financial information.

Since January 2020, more than 4,000 COVID-19-related websites have been registered, 3% (120) of which are malicious, and another 5% (200) suspicious. Coronavirus- related pages are 50% more likely to be malicious.

2: Well-crafted clone websites. A number of fake websites disguising themselves as official international aid and public health organizations, such as the World Health Organization (WHO) and the Center for Disease Control (CDC).

The WHO is one of the most common hijacks in current spam campaigns. The WHO itself corroborates our BlackPot findings. According to the WHO, threat actors disguise themselves as one of their agents, in order to obtain sensitive information or direct donations via emails, phone calls, text messages, or even fax.

The Canadian Red Cross, again correlating our data, is also warning people not to click on links claiming to come from them, offering face masks. Cybercriminals send malicious links disguised as important information that install malware, and then they steal personal or login information when clicked.



EXAMPLES: Malware, App, Spam Scams Most Commonly Used

► A COVID-19 malspam campaign targeting the manufacturing, industrial, financial, transportation, pharmaceutical, and cosmetic sectors. Hackers used Microsoft Word documents that exploit a well-known (to hackers) Microsoft Office vulnerability, in order to install **AZORult** malware. **AZORult** steals information, and has also been distributed through a fraudulent version of the Johns Hopkins University of Medicine's Coronavirus Map.

► Other malware programs leveraging COVID-19:

The **Emotet** virus (also uses Word documents), **Nanocore RAT**, and **Parallax** activity have increased since the outbreak. These malware programs are particularly penetrating, and can be used for remote access, keylogging, stealing files, accessing webcams—all in addition to downloading and opening files.

► A fake, real-time COVID-19 tracker android application, **"COVID19 Tracker**", infiltrates user permissions, changes a phone's screen lock password, installs **CovidLock** ransomware, and demands $100 in Bitcoin in exchange for restoring files.

► University attacks. A phishing attack targeting students and university staff using fake emails to steal Office 365 login credentials. This sort of scam, leverage widespread use of remote classrooms, exemplifies a problem that makes individuals most vulnerable.

► Spamming attacks on websites. People think they are linking to COVID-19 updates, but instead are directed to drug-dealer sites.

► New spam campaign that plays on the face mask shortage, and steals money from purchasers.

Attacks on government agencies

Government agency vulnerability is at an all-time high because all

decision makers, on both local and national levels, are fully focused on slowing the spread of the virus. An attack on a state institution can cause enough damage that adversarial governments, or other state-sponsored terrorist organizations, can infiltrate.

- The US Department of Health and Human Services (HHS) suffered several cyberattacks that attempted to slow down their system. HHS servers were overloaded for hours as a result of the attack. Hackers do not appear to have stolen any data, as of the date of this report. US officials suspect the attacker was foreign, but there is no definitive evidence. However, there are indicators that the attackers may have served a foreign nation's interests. According to U.S. press reports, hackers did attempt to test the HHS security systems. The incident turned out to be a particularly aggressive attempt, as the attackers searched for vulnerabilities in the network and possibly tried to break into email servers. Investigators are also assessing whether there is a link between messages announcing the nationwide quarantine and this series of attacks. Our data does establish such a link.
- Hackers attacked a hospital in Brno, Czech Republic, obstructing publication of many COVID-19 tests results, days after the national emergency was declared. The attack specifically targeted the health sector.

The APT hacker group, which has been previously linked to China, attempted a targeted cyberattack against a Mongolian public sector organization using sophisticated offensive tools that exploited the panic around COVID-19.

The APT group sent two documents that were disguised as Mongolian Ministry of Foreign Affairs press releases. The social engineering campaign sought to deliver unique remote access malware infected documents.

APT36, a Pakistani state-sponsored offensive group, targeted Indian government embassies. They launched a spear-phishing campaign using a COVID-19 health advice document as bait, which installed the Crimson Remote Administration Tool (RAT) on the embassy's systems.

- Researchers uncovered a malware campaign launched by North Korean hackers that used South Korea's response to the epidemic as a trap.
- Disguised e-mails, infected with trojan viruses, targeted Ukrainian addresses and looked like they were sent by the Public Health Center of the Ukrainian Ministry of Health. They contained the latest news about COVID-19, but also delivered hidden malicious content. The emails appear to have been part of a larger disinformation campaign targeting the entire country on various fronts. The organization suspected of perpetrating the campaign is the APT28 (Fancy Bear) group, closely linked to Russian state intelligence.

Critical infrastructure is at stake. All of the above attacks take advantage of, and build upon, the conditions that COVID-19 create, according to *CIM* ICS-specific CTI system data.

THE ANALYSIS OF FINDINGS:

Analysis of data from the *CIM*-CTI system

The CIM-CTI system is a data collection system focused on industrial controllers. It collects the widest possible range of information about attacks, attack methodologies, and attack vectors against worldwide industrial controllers.

We collected all COVID-19 related data from our system, focusing on the following three key areas:

- Social media platforms
- BlackPot data
- Dark web

The results:

Social media platforms

Under the umbrella term CTI activities, the CIM system automatically collects focus-oriented data. The data is centered around cyber security, particularly industrial controllers. From December 2019 through March 2020, there has been a noticeable increase in the number of entries mentioning COVID-19, as well as the number of cyber-attacks with relation to the pandemic.

CTI INCREASES

COVID-19-related SOCIAL MEDIA entries in accounts increase to 1,500 in January. In February they increase to more than 4,000 and by the end of March we see more than 7,000 entries.

HACKING RELATED ENTRIES: combining the words “coronavirus” and “hacking”:

The number of social media entries in the system specifically related to generic hacking (*without* the mention of coronavirus) has been declining since December 2019. In detail this means that, while in December we found almost 20,000 entries, by January we only had around 15,000. By February and March, these numbers fell further: 5,500 entries in February, and around 3,000 in March.

This tendency specifically has nothing to do with the COVID-19 outbreak.

However, the first entry we detected on social media combining the words “coronavirus” and “hack” happened in January. The number of entries grew to five by February 13th. In March, this number surged, with 275 entries by March 18th. On March 6th and March 16th alone, we saw 88 and 79 new entries respectively. (The reason for the latter is that the US HHS Secretary-General released a press statement on March 16th, announcing a complex cyber security attack, presumably perpetrated by foreign state actors.)

Combining these two statistics reveals that almost 10% of all hacking-related social media entries were about COVID-19 linked cyber-attacks in March.

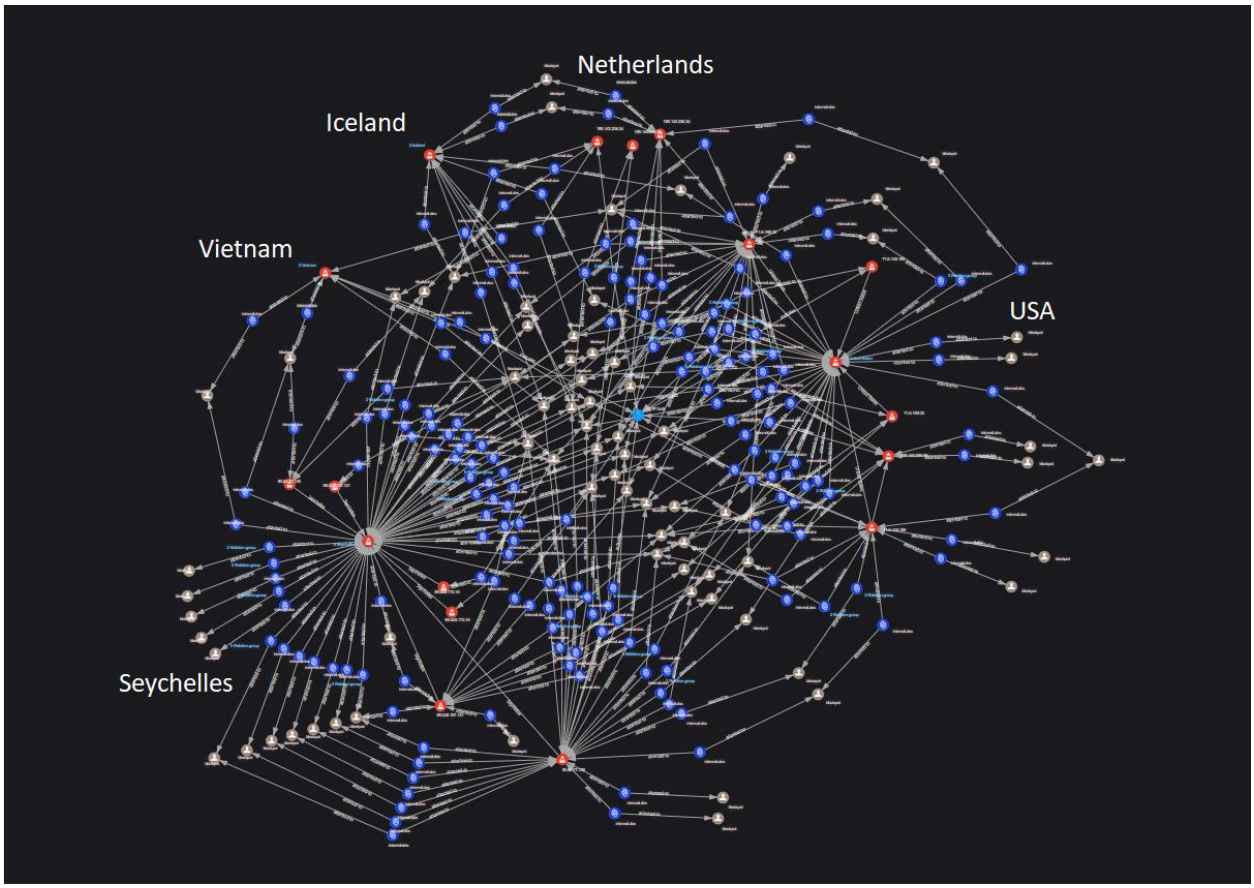
The data shows that the percentage of COVID-19-related attacks will continue to increase, with the critical infrastructure of governments specifically at risk to be attacked by an increasing number of threat actors.

This conclusion is reinforced by the fact that our data source in CIM is a CTI system optimized specifically for ICSes and critical infrastructure.

This trend also shows that the spread of the virus is increasing the security risk to critical infrastructures. This is also supported by data collected from *CIM* BlackPots, the hundreds of mostly ICS-specific honeypots, which have been deployed worldwide for targeted data collection.

Analysis of BlackPot data

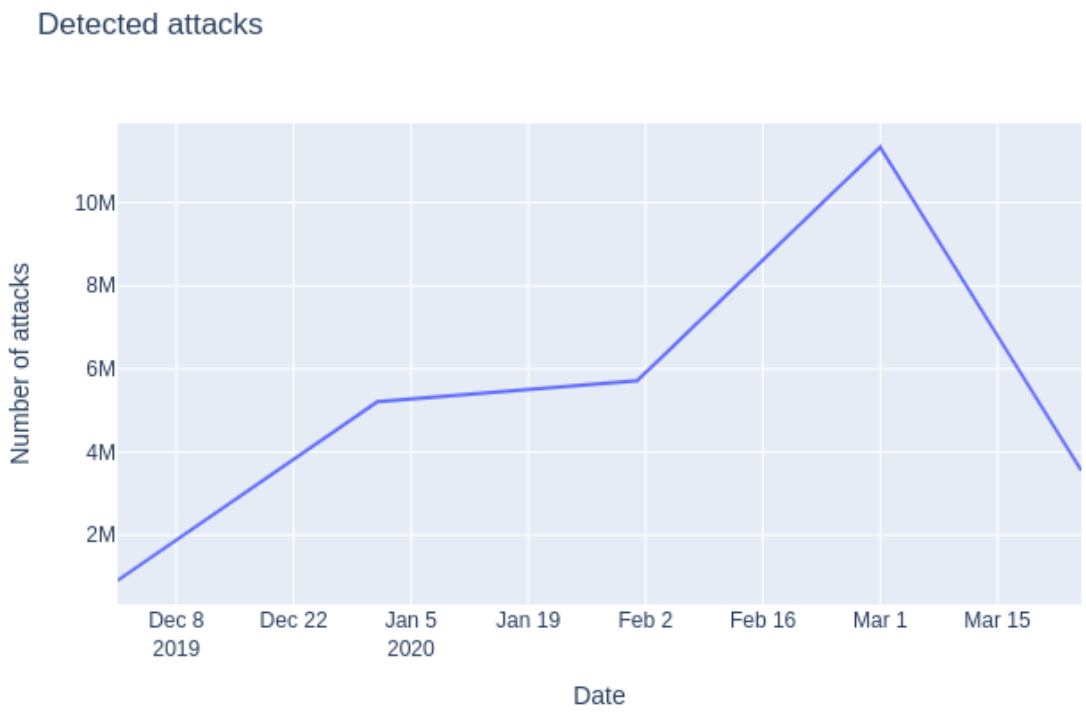
We used a dual approach to analyze BlackPot data. 1) We investigated the direction of attacks. 2) We examined the attacked tools at regional level.



Analysis of attacks by the direction of attacks:

We have detected 26,730,000 attacks since November 2019. The first COVID-19 patients appeared in China in November. Since November, the monthly attacks have been steadily increasing: 11,300,000 occurred in February, when COVID-19 became a true pandemic. Examining only the numbers, there is a clear correlation between the numbers and the spread of the virus.

Even more telling is the local and country-by-country analysis of the data, taking into account the virus situation in the area.



Asia and China

November 2019: 250,000 attacks from the region are detected, of which slightly less than 50% are linked to China.

December 2019: The number of these attacks exceeded 1,700,000 (a 600% increase), and China-specific attacks increase to 831,000.

January 2020: 2.5 million attacks regionally, with more than 900,000 in China.

Please note that the pandemic peaked in China in January. In the light of that, the figures in February are compelling:

February 2020: more than 4.2 million attacks. However, the number of Chinese attacks decreased to 860,000--approaching the number of cases in December 2019.

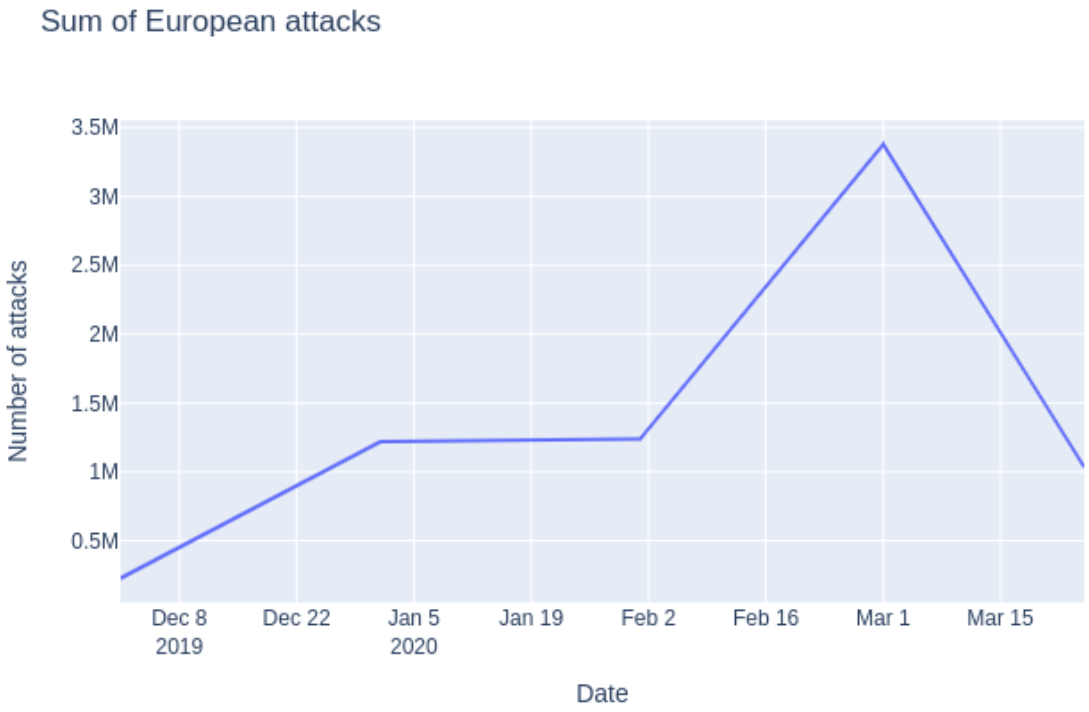
South Korea

Examining South Korea, the data verifies the pandemic's course. In South Korea, the virus reached its peak by February, just after the effects of the epidemic in China seemed to ease. Our country-related data correlates. In December 2019 and January 2020, roughly the same slight growth figures are reported, with approximately 190,000 monthly attacks.

February 2020: monthly attacks are more than 800,000. In South Korea, where the pandemic was still peaking in February – unlike in China – the number of attacks continues to increase in line with the regional virus spread.

European Union (E.U.) countries

The same patterns can be observed in the E.U. By February 2020, the pandemic caused affected countries to introduce specific laws and extraordinary measures. Our data of attacks for February also showed a dynamically growing trend. The number of attacks from Europe increased from 1.2 million in January 2020 to 3.4 million in February 2020.



Broken down by countries, the attacks are greater for countries affected severely by the virus.

ITALY: January 2020, 123,000 attacks.

February 2020, 375,000.

SPAIN: January 2020, 30,000 attacks.

February 2020, 116,000.

However, in countries with fewer virus-related state initiatives, the number of attacks didn't increase as much.

Sweden

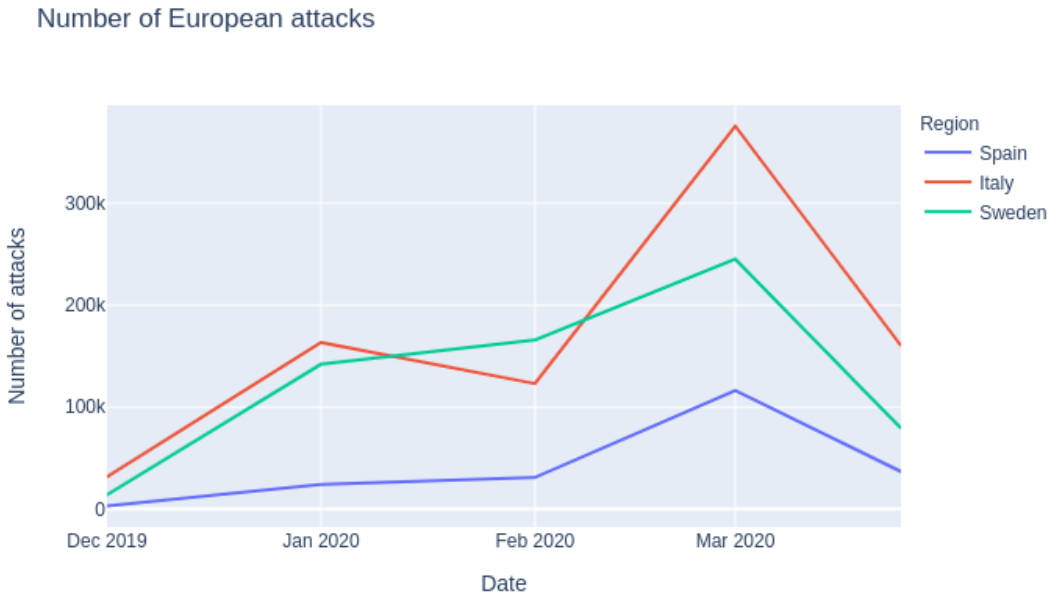
In Sweden, neither the state, nor the public, responded to COVID-19 on the same scale as other E.U. countries.

January 2020, 165,000 attacks.

February 2020, 245,000. This is a 47% increase, versus the 277% increase in Spain, and 205% increase in Italy.

The data clearly shows that as the virus situation in a given country increases, the country-specific cybercrime activity also increases.

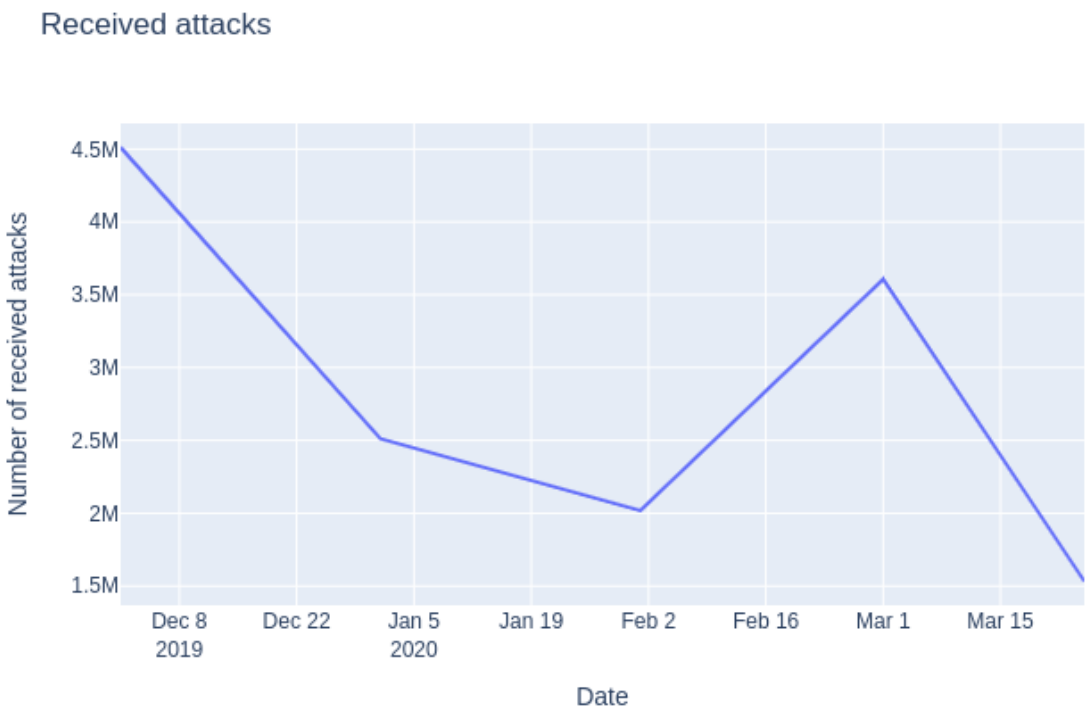
While many attacks may be symptomatic of a global tendency during a pandemic, local intel can also be gleaned, either at individual or state level:



Corporate infrastructure has become more vulnerable, as attacks may go unnoticed. It is possible that more attackers will move to take control of machines and networks, including corporations. But it is also possible that the attacked infrastructure of an otherwise vulnerable country will be slowed down by efforts to overload central gateways. An increase in state-sponsored malicious activity may also be detected in such cases.

Analysis of data generated during attacks

During our study, we focused on three regions, and several countries within those regions, from December 2019 through March 2020. We detected 17 million attacks on our CTI tools in Asia, Europe, and the United States.



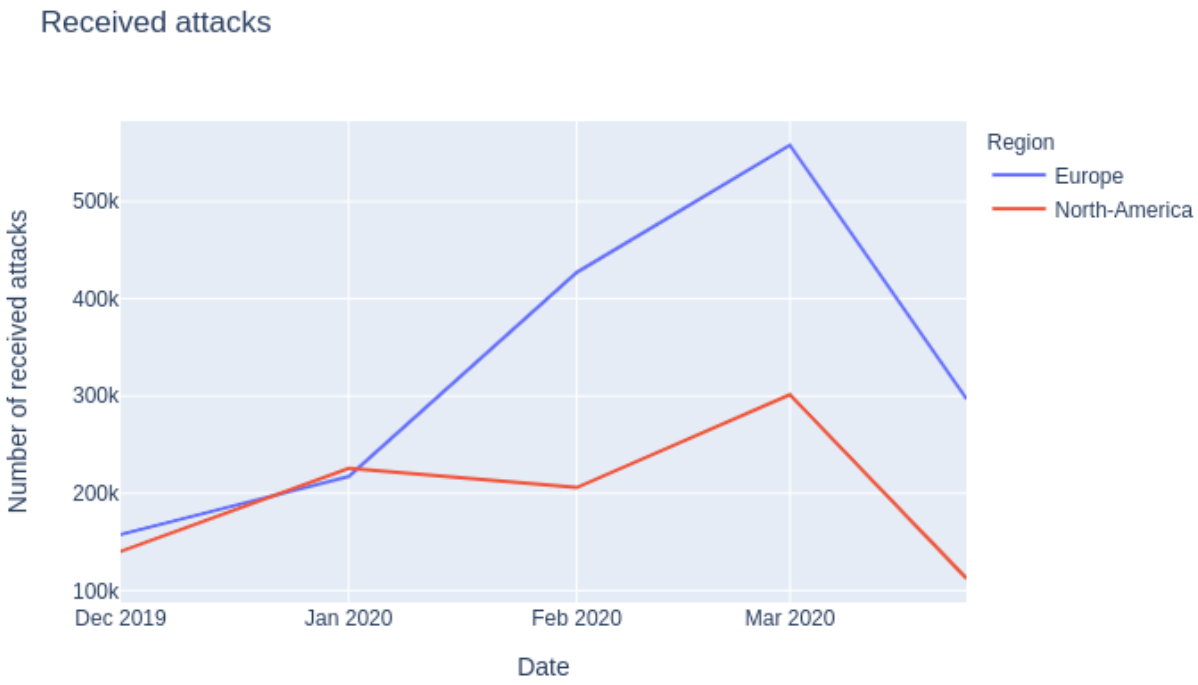
Europe

In Europe, COVID-19 turns pandemic in February, and the attack data expands in step. In France, the number of detected incidents in January 2020 is 1,200,000, lower than in December 2019. But in February 2020, it increases to nearly 2,300,000. The number of attacks in England also increases in February compared to January. The correlation between the measures taken by the country and the increase in the number of attacks is clear: In France, serious state-level measures are in place to stop the spread of the virus by February, while in the United Kingdom it is not until March. Our data matches those trends. From January to February in France, the rate of attack growth is above 80%, compared with 30% in the United Kingdom.

United States

In the United States, a profound increase in attacks on our tools can be detected by February 2020.

Here, too, the figures significantly exceed the relatively high figures for December. The correlation between the rate of attack increase, and the steps taken by the federal and state governments, can also be observed here. In the United States, although the presence of the virus is already noticeable in February 2020, government responses do not attach much importance to it, and the number of attacks detected is “only” a 40% increase.



Asia

In Asia, the patterns of documented attacks are similar to the E.U. and the United States. In South Korea, which has already been analyzed here from another perspective, nearly twice as many attacks (nearly 10,000) are detected by our tools in February 2020 than in January 2020.

Regardless of region, the number of attacks on each country increased significantly with the appearance of, and reaction to, COVID-19. Because the more a country was infected, the more it was attacked, therein lies the future cybersecurity challenge: The countries more vulnerable to the pandemic are now prime targets for cybercriminals.

SUMMARY:

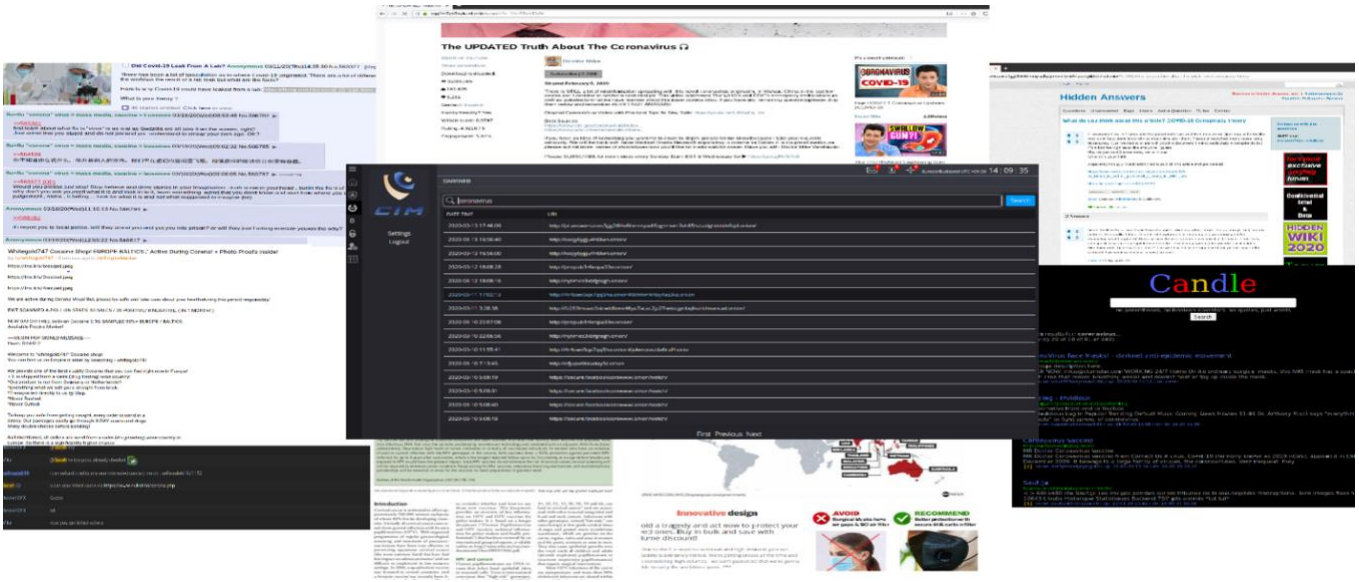
- BlackPot data shows a tremendous increase in calculated and aggressive attack activity globally over the last three months.
- Simultaneously, the number of incidents affecting the CIM toolkit increased in step.

* Both the offensive activity, and the number of attacks, are proportionate to the presence of COVID-19, its severity in a country/region, and the government response.

- The greater the exposure of a country to the pandemic, the greater the exposure of its network infrastructure and cybersecurity tools.

Dark web

We also conduct targeted data collection in subject-specific areas, such as the Dark web. The same patterns can be observed on the Dark web as on the clear Web:



After analyzing the available entries containing the words cornavirus, covid, hack, hacker, attack, etc., we discovered that the number of topic-specific posts on the Dark web is increasing exponentially as well: 4 such entries in December 2019, 314 in January 2020, 2,300 in February 2020, and more than 3,000 by mid-March.

Dark web specifics:

► Posts centering around health-related protective equipment have been published on various forums throughout the Dark web. This is also confirmed by figures in our system, as the number of entries containing the words “mask” and “virus”, as well as the word “hand disinfectant,” has grown exponentially during the analyzed period. We found several places selling protective masks, and even a place that specifically sells stolen masks. In many places, they also sell various drugs and vaccines that claim to be effective against the virus. As with all fraud campaigns, these are almost exclusively aimed at stealing money. There are some slightly more sophisticated sellers of fake vaccines who make reference to otherwise real companies that are engaged in vaccine development.

► We also identified an entry where the virus itself was being offered for sale.

► There are also entries we identified, where entities were looking to purchase virus tests.

► We have found drug selling sites that mention THC as a possible cure for the virus in an attempt to boost demand.

► A specifically virus-themed Webshop was also created.

► There are many dedicated virus topics on most forum pages, suggesting that the scams are still in full throes.

► The many extremist groups on the Dark web are also concerned with the pandemic. The Daily Stormer, an American neo Nazi

group, has published two articles on its site, while an anti-NATO, Far-Left-Wing organization that is likely under Russian influence, has also petitioned for the cancellation of European NATO military exercises related to COVID-19 set to take place in 2020.

► Many news articles and posts related to the virus are circulating on the Dark web, which can clearly be identified as misinformation or plain fake news.

We can confirm that the COVID-19 pandemic has a clear impact on cyber security. With the spread of the virus, both individuals and governmental entities are more vulnerable for a variety of reasons that require immediate intervention and remediation.

As the virus takes its toll globally, the number of cyber-attacks attempting to exploit the situation will also increase accordingly.

Attackers will target individuals, who may become victims because of curiosity and fear. The attackers will use the situation to create fraudulent campaigns in order to steal sensitive information and money.

Governments, especially ones severely affected by the pandemic, are becoming targets.

Fraudulent entities may exploit the weakened state of organizations for future campaigns.

Their goal: To target them specifically, using highly sophisticated and complex methods, in order to further reduce defensive capabilities.

Infrastructures using industrial controllers and other critical infrastructure tools are more vulnerable to attacks. Forecasts and historical data suggest that this trend will only increase as the response to the pandemic grows.