TLP: GREEN

Are Dark Web and Deep Web Hotbed of Hackers?

AhnLab Contents Planning Team

2022. 06. 07

AhnLab

Guide on Document Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Notices
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can be only accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded,
meaning that the sum of each item may not match the total.

The version information of this report is as follows:

Version	Date	Details
1.0	2022-06-07	Are Dark Web and Deep Web Hotbed of Hackers?

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report
may change without notice if new evidence is confirmed.

Overview

The new Cold War between the United States and Russia along with Russia's invasion of Ukraine during the first quarter of 2022 left deep impacts on both the physical and the cyber world. The identity of Conti group, which was once one of the most active ransomware group, was revealed with their source code. Many members of the infamous REvil ransomware group were arrested and multiple underground forums have been shut down. However, crimes using Dark Web and Deep Web continue to persist. How is that this market is maintaining an ecosystem similar to that of a normal business? The answer lies in the endless demands and usability.

AhnLab will discuss the recent trends of Dark Web and Deep Web, based on ransomware, black markets, and hacking groups.

Are Dark Web and Deep Web Hotbed of Hackers?

Previously, people thought that the Dark Web was merely used only by cyber criminals and hackers. But according to KISA (Korea Internet & Security Agency), about 15,000 people access the Dark Web daily.

Before we get into the details, let's find out more about the difference between Dark Web and Deep Web.

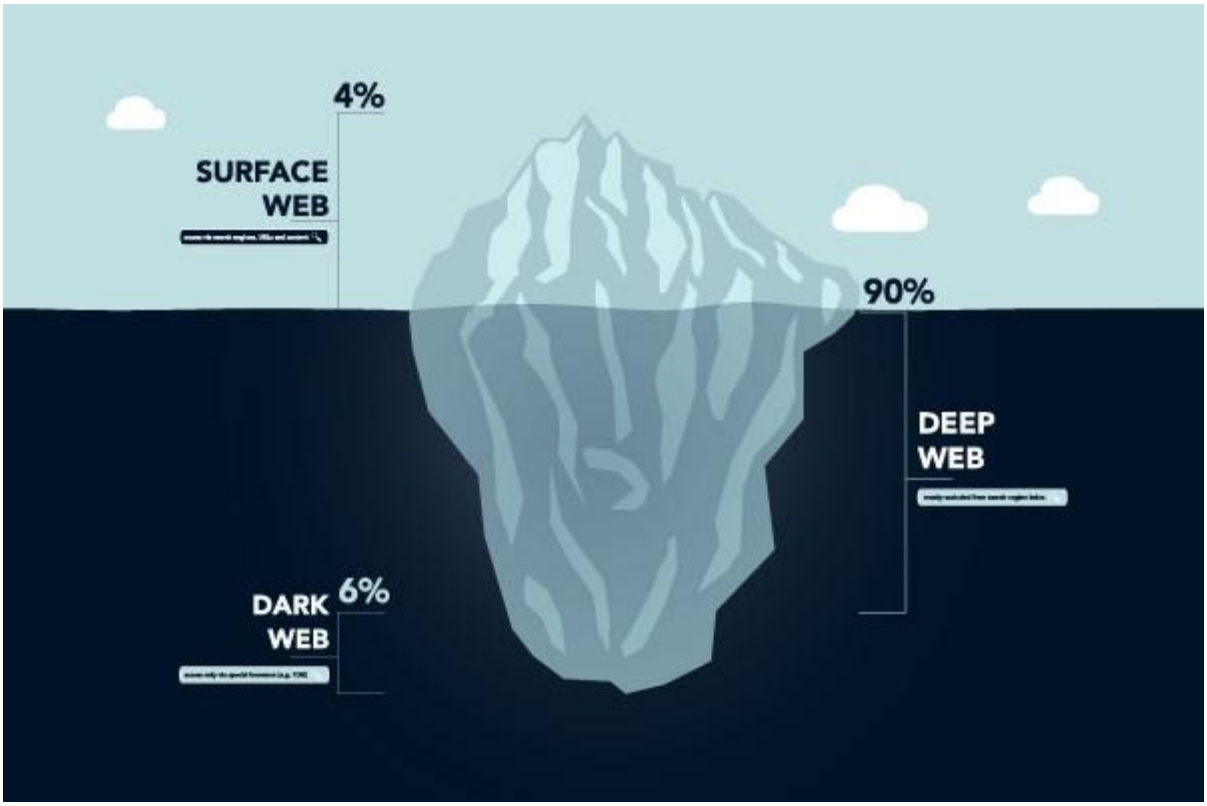


Figure 1. Structure of the Internet World: Surface Web, Deep Web, and Dark Web

Understanding the Difference between the Dark Web & Deep Web

Dark Web is sometimes called as Deep Web, but the two are not exactly the same. Deep Web refers to all webpages that cannot be found using search engines, taking up between 96% to 99% of the entire Internet. Dark Web is a subgroup of Deep Web that is intentionally hidden

and can be accessed through specific browsers. This takes up about 5% of the entire webpage.

Not all Dark Webs are used for illegal purposes, but most of the time, ransomware and hacking groups exploit them for malicious activities.

Main Issue #1: Ransomware

Ransomware groups avoid various sanctions through continuous rebranding. The most notable example is ALPHV. It is assumed that one person is behind the creation of ransomware, known as ALPHV or BlackCat. To rebrand their identity, the creator actively recruited people from various ransomware groups, such as REvil, DarkSide, BlackMatter, and Maze.

- Rebranding Order: DarkSide → BlackMatter → BlackCat (ALPHV)

Figure 2. Webpage of ALPHV Ransomware Group

Recently, many ransomware groups are attempting to rebrand their identity. As the names are constantly changing, it can be assumed that the ransomware ecosystem is smaller than we know.

Another example is Conti ransomware. Conti is known as a rebrand of Ryuk ransomware, which have attacked more than 800 organizations worldwide.

Figure 3. Webpage of Conti Ransomware Group

The group's chat history as well as source codes and tools for ransomware encryption and decryption have recently been leaked. Yet the group shows no diminished activities. Since RaaS (Ransomware as a Service) has an ecosystem that is similar to a normal business, the data breach incident does not seem to affect the group's operation.

Another noticeable trend among ransomware groups is having a separate website for ransom negotiation. For instance, Hive group has a PR webpage showing the list of victims and a webpage for negotiations.

Figure 4. Operation webpage (left) and negotiation webpage (right) of Hive

In order to negotiate the ransom amount, the user needs an onion address, mentioned in the ransom note, and the login account credentials. The group recently increased the default ransom from 1.2 million dollars to 2 million dollars, and updated their ransom note.

While some groups have separate webpages for negotiations, others made their ransomware operate in new environments, such as Linux. For example, LockBit has variants that can now operate in Linux and ESXi environments.

MD5	V3 Alias
3c9e550d41f3de930e678776a6e018ed	Ransomware/Linux.Generic.260872
9661c01af31a41caef2ccd3b6be06e60	Ransomware/Linux.Generic.259496
18a352d33c8c01b6a196adce176c5a96	Ransomware/Linux.Generic.252680

Table 1. Linux variants of LockBit

LockBit was just as active as Conti, having almost similar amount of victims; there were over 500 victims as of January 2022. The group listed a new list of 14 victims in the middle of February. In the middle of March, it again listed a list of 22 new victims in just 2 days.

There were also ransomware groups that took a different route. Some suddenly declared retirement or had their operation shut down due to having key members arrested. The person who is assumed to be the creator of Maze ransomware revealed the master keys of Maze, Egregor, Sekhmet through the BleepingComputer.com forum. Based on the revealed keys, security company 'Emsisoft' created a decryption tool.
- Link: https://www.emsisoft.com/ransomware-decryption-tools/maze-sekhmet-egregor?__c=1

Figure 5. Emsisoft's Decryption Tool for Maze/Sekhmet/Egregor

The reason why the creator of Maze or admin of a black market would retire may be due to various personal reasons: being arrested or the fear of being arrested, rebranding, accomplishing financial goals, or personal health issues.

Some groups were arrested before the members could retire. The group known for GandCrab, later rebranded as REvil and Sodinokibi, had their members arrested in January, 2022.

Yet surprisingly, some members of the group are still known to be active. There is a rumor that the group is still active with a new brand beacuse those those arrested were merely pentesters or affiliated people.

Table 2 shows the timeline for REvil collaborators who were arrested in 2021.

Date	Details
February, 2021 April, 2021 October, 2021	3 REvil and GandCrab collaborators arrested in the Republic of Korea
November, 2021	2 REvil collaborators arrested in Constanta, Romania
November, 2021	1 GandCrab collaborator arrested in Kuwait

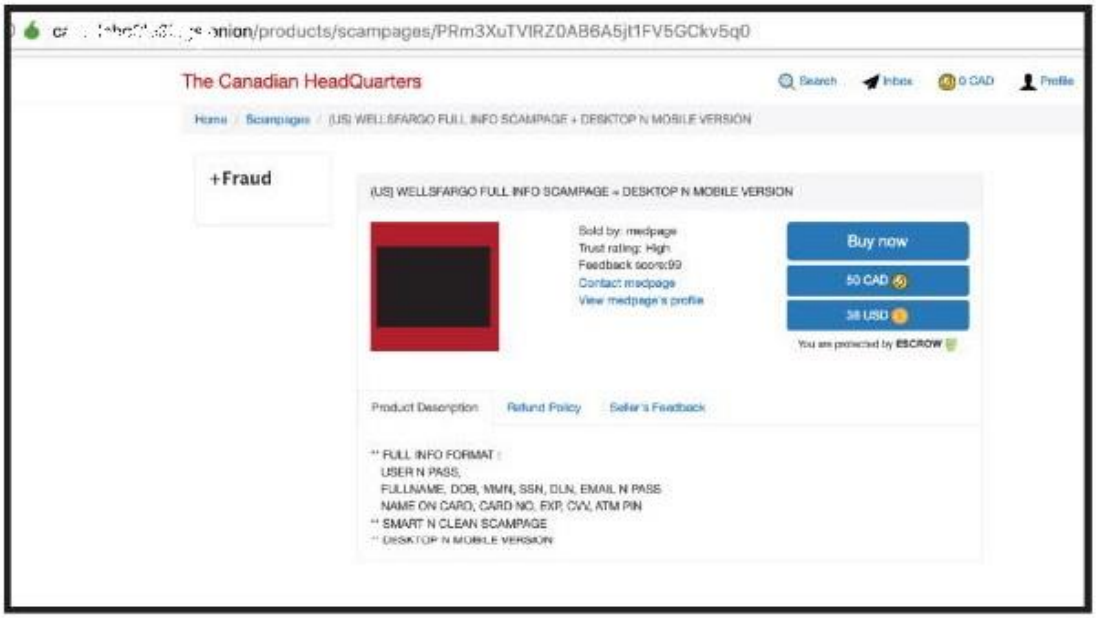
Table 2. Timeline for REvil collaborators arrested in 2021

Main Issue #2: Forums and Black Markets

Forums and black markets have undergone many changes after government organizations sought to tighten their grip on them. Some were shut down by government organizations or law enforcement agencies, while others voluntarily retired or exit scamming.

1. Shutdown of Black Markets (ex. CanadianHQ and Monopoly Market)

Canadian HeadQuarters (CanadianHQ), which was active since 2018 was shut down by the Canadian government. Canadian HeadQuarters (also known as CanadianHQ) is a Dark Web marketplace that is relatively well-known. It traded fraud, drugs, spam services, phishing kits, verifications for stolen credentials, and access information for compromised computers. The government released the names and nicknames of 4 administrators in black market and imposed fines on them.



Screen shot of a stolen Wells Fargo customer's credit card advertised on the Canadian HeadQuarters site. Image from a Terbium Labs report in 2020

Figure 6. CandianHQ (Reference: Terbium Labs Report in 2020)

Monopoly Market is the oldest Dark Web marketplace that had been operating since 2019, are associated with illegal drug trade. While the exact reason for shut down is unknown, it is likely the admin of the website chose to shut down the webpage due to the fear of being arrested or have already reached their financial goal.

Figure 7. Monopoly Market

2. Raid Forums Access Denied

Raid Forums is well-known for leaking DBs (databases). However, access to the website has been denied since mid-February. It was one of the biggest hacking forums in the world with over 500,000 users.

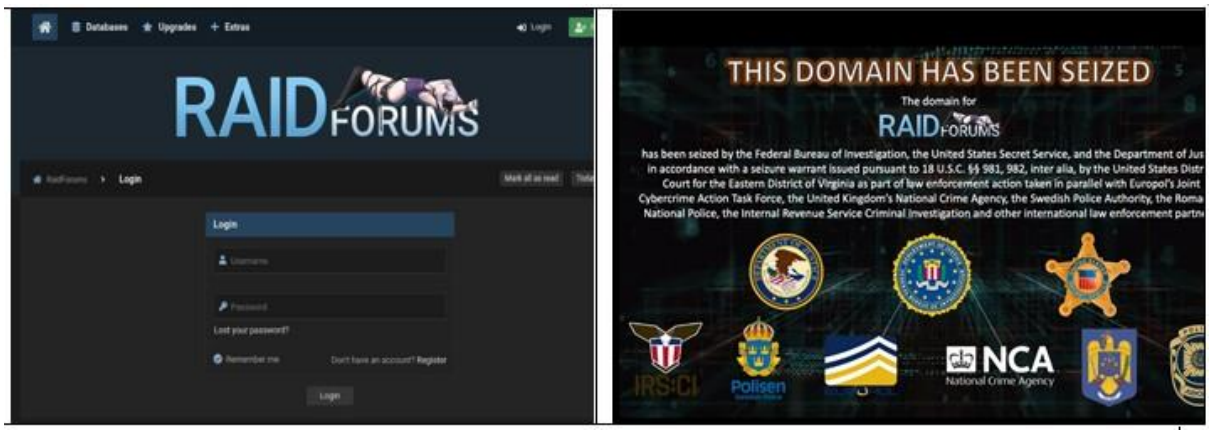


Figure 8. Raid Forums login page before it closed down (left), their domain currently seized by law enforcements (right)

The US Department of Justice cooperated with law enforcement agencies of England, Sweden, Portugal, and Romania to close down the forum. The creator who was also the admin of the forum was arrested in England on April 12th, 2022. The domain is currently seized by the US Department of Justice.

3. World Market's Exit Scamming

World Market, which was active since November 2020, is recently under suspicion of engaging in exit scamming. It is a marketplace on the Dark Web that provides the escrow service of storing the fund until the order is processed. Recently, the service is experiencing issues, as shown in Figure 9.

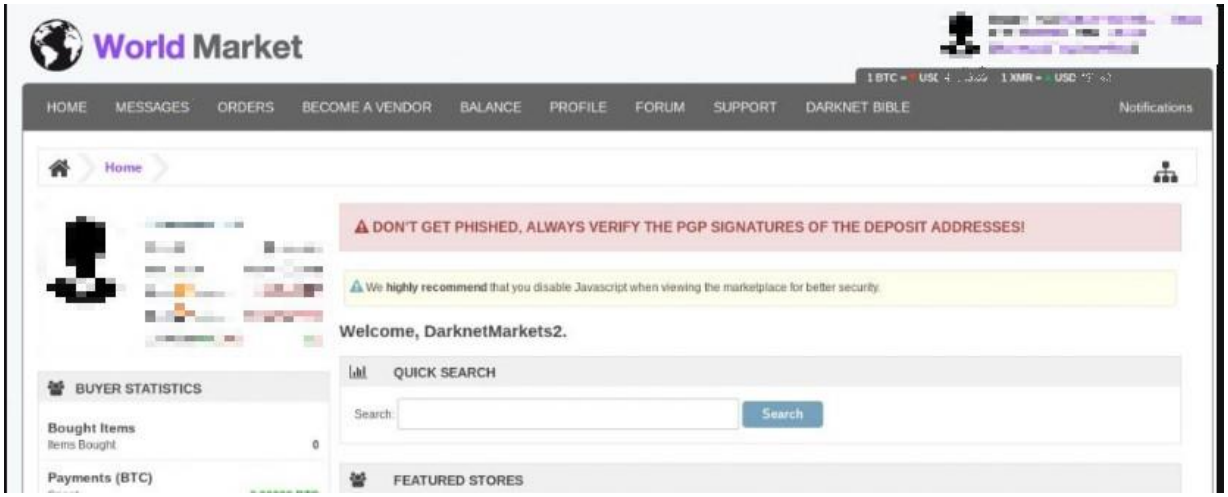


Figure 9. Displayed page when logged in to World Market

The issues include users' cryptocurrencies disappearing, withdrawals being delayed, and only a small amount being withdrawn.

4. Shut Down of SkyFraud and Ferum

SkyFraud and Ferum, relatively huge forums selling stolen credit card credentials (also known as Carding Forums), closed down.

Figure 10. Main page of SkyFraud seized by the BSTM-K group of the Ministry of Internal Affairs of the Russian Federation

Two more forums were shut down by the operations that were presumably carried out by the same group. It left a message 'Who will be next?' in Russian on the main page of SkyFraud, foreshadowing follow-up arrests of cyber criminals in Russia.

Main Issue #3: Hacking Groups

There was also news of hacking groups being shut down. In January 2022, NetWalker ransomware group was shut down due to cooperation between the United States and Bulgarian governments. A Canadian man who was known to be an affiliate of the group was sentenced to 80 months in prison and had his cryptocurrencies (719.99 BTC and 15.72 XMR) seized.

Messages sent between Conti ransomware group members were leaked by a security researcher living in Ukraine. According to the leaked information, GOLD BLACKBURN group and GOLD ULRICK group make up the group.

GOLD BLACKBURN is a cybercrime group with financial aims that started their activities since June, 2014. They created and operated TrickBot malware from late 2016 to March 2022. They also distributed various malware types, such as BazarLoader, Anchor, Zloader, and Buer Loader.

On the other hand, GOLD ULRICK is solely focusing on ransomware attacks, and they have been active since the mid-2018. The group distributed Ryuk from August 2018 to early 2021. They distributed Conti after going through a rebranding in early 2020.

There was also a case of the LAPSUS$ group, which targeted companies globally. One example includes hacking Okta to leak sensitive customer information. It is said that the incident started from Sykes Enterprise, a third-party company for customer support. Since customer support companies have a wide range of access permissions to carry out customer requests, they are often the target of hacking groups.

Conclusion

Cybercrime organizations in the Deep Web and Dark Web have ecosystems similar to that of normal businesses. There are two reasons for the continuation of the business: the increasing demand and usability of the market.

Dark Web market business is functional even when the buyer and the seller is physically distant. One can try RaaS (Ransomware as a Service) for ransomware and MaaS (Malware as a Service) for malware. The market offers a centralized service connecting buyers and sellers. It is also equipped with a user-tier service and the escrow service, which stores funds until orders are processed. Besides the ease of using the service, the high profitability contributes to the increase of cyber criminals using the Deep Web and Dark Web for malicious intentions.

The global cooperation to actively crack down cyber criminals who are active on the Dark Web and Deep Web continues as many are keeping a close eye on the behaviors and changes displayed through the attack methods.

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
www.ahnlab.com
www.asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency Response Center(ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. The ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab