The Rise & Demise of Multi-Million Ransomware Business Empire

advanced-intel.com/post/the-rise-demise-of-multi-million-ransomware-business-empire

AdvIntel June 15, 2021

- Jun 15, 2021
-
- 10 min read

Vitali Kremez & Yelisey Boguslavskiy

Executive Summary:

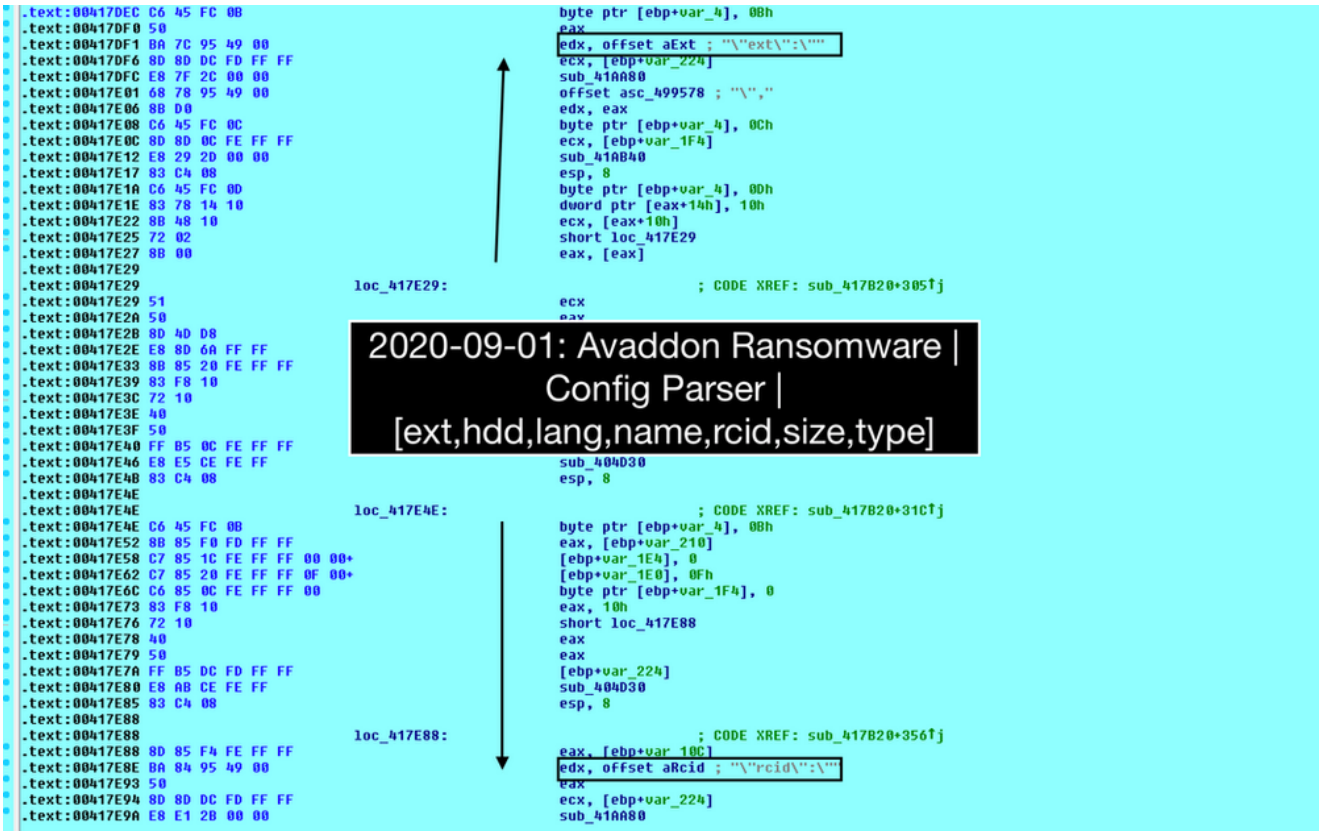
- On June 11, 2021, Avaddon ransomware responsible for numerous cyber incidents since 2020 made a decision to not only suspend their operations but provide decryption keys for all the victims who were targeted by them.

- AdvIntel was able to achieve unmatched visibility into the Avaddon victimology by obtaining their Master Key information. This visibility into all victims of the group (and not only companies whose data was officially dumped on Avaddon's shame blog) enabled unique insights into Avadon's patterns, strategies, and methods.
- Through investigating victimology, AdvIntel assessed that the total income made by one operator through the year of Avaddon activities could potentially equal 1,000 Russian median salaries which explains the foundation of ransonomics and why it attracts more and more talented individuals in Russia and other states.
- According to unique AdvIntel findings obtained through exhaustive investigations of the Russian-speaking underground cybercrime community, Avaddon demise was likely caused by political reasons - a sharp reaction of the US presidential administration on the recent ransomware attacks, and the subsequent pressure applied by Russian law enforcement against local cybercrime groups prior to the upcoming Bide-Putin summit.

Introduction - The Lost Empire

The three-letter Hebrew root "**avad**" (אבד), from which the name is Avaddon derived, has two main semantic interpretations- "to destroy" and "to lose / get lost". Indeed, these two meanings perfectly define the Avaddon ransomware - a destructive and malicious force - which always managed to conceal itself and disappear.

Today we shed light on this lost and hidden criminal empire using unique datasets - the full list of Avaddon victims ever targeted by the group over the year of its existence - discovered by AdvIntel. This unique **SIGINT** data is supported by exclusive **HUMINT** findings - statements made by the Eastern-European underground cybercommunity leaders who worked with Avaddon - explaining and interpreting the groups' rapid rise and even more rapid downfall.

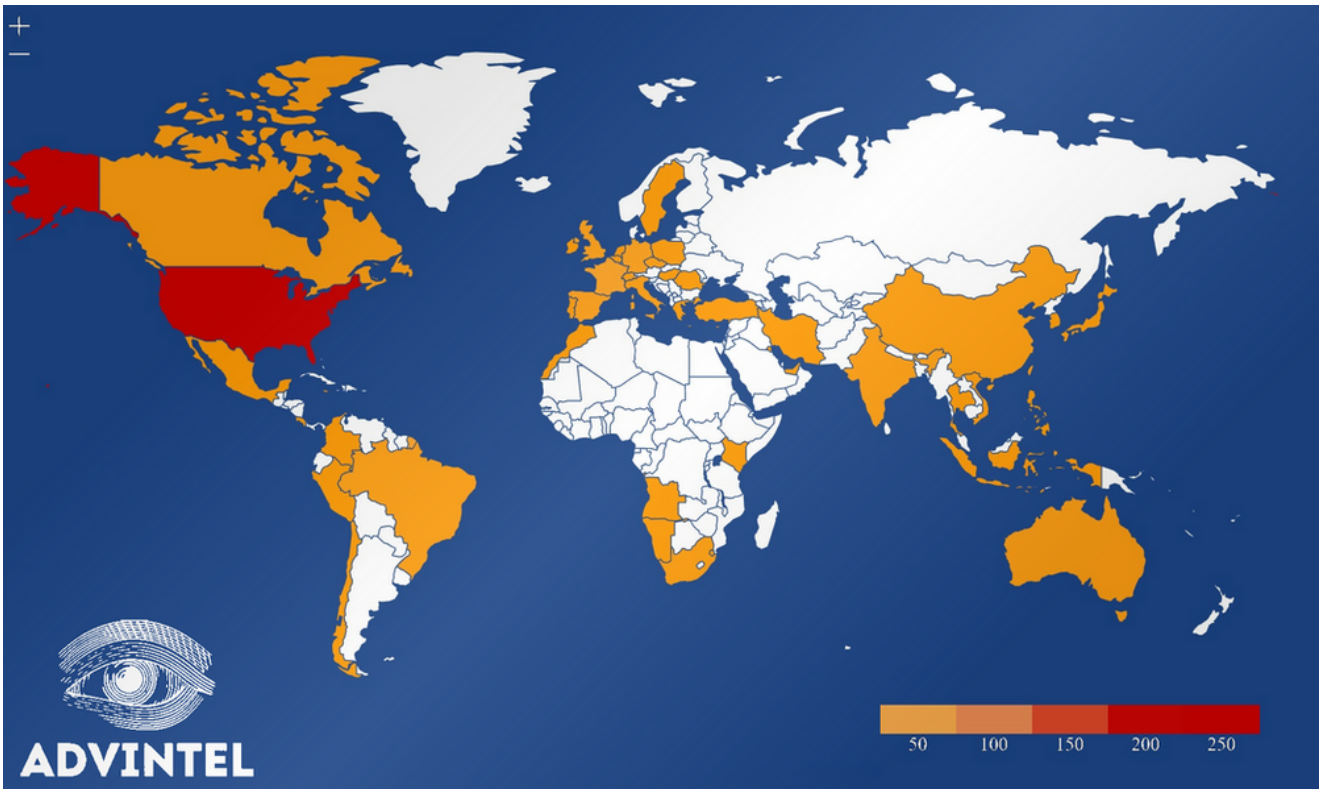


Avaddon & The Birth of "Ransonomics"

On June 11, 2021, Avaddon released keys for over 2,000 victims containing the exact company breach names.

Our analysis of the confirmed victimology shows that some of them were the world's leading companies. How did this group succeed in hitting so many companies within a year? The answer is - Avaddon created an entire ecosystem around themselves - a web of supply chains**,** international affiliates, sellers, underground auction managers, and negotiators. They have established an organic ecosystem of criminal extortion economy - a form of "**ransonomics**."

Of course, Avaddon was not the only group pursuing a diversified approach to building a larger business system. However, they were likely the most creative ones. They were the only Russian-speaking group that enabled but promoted international partners joining the team as affiliates that directly represented the coverage of Avaddon's attacks, reaching five continents.



Avaddon operations targeted companies and governments all across the globe, with the exception of Russia

One of Avaddon's largest attacks - on a major financial institution occurring in May 2021 - illustrates this integrated approach of building the ransomware-attacks economy.

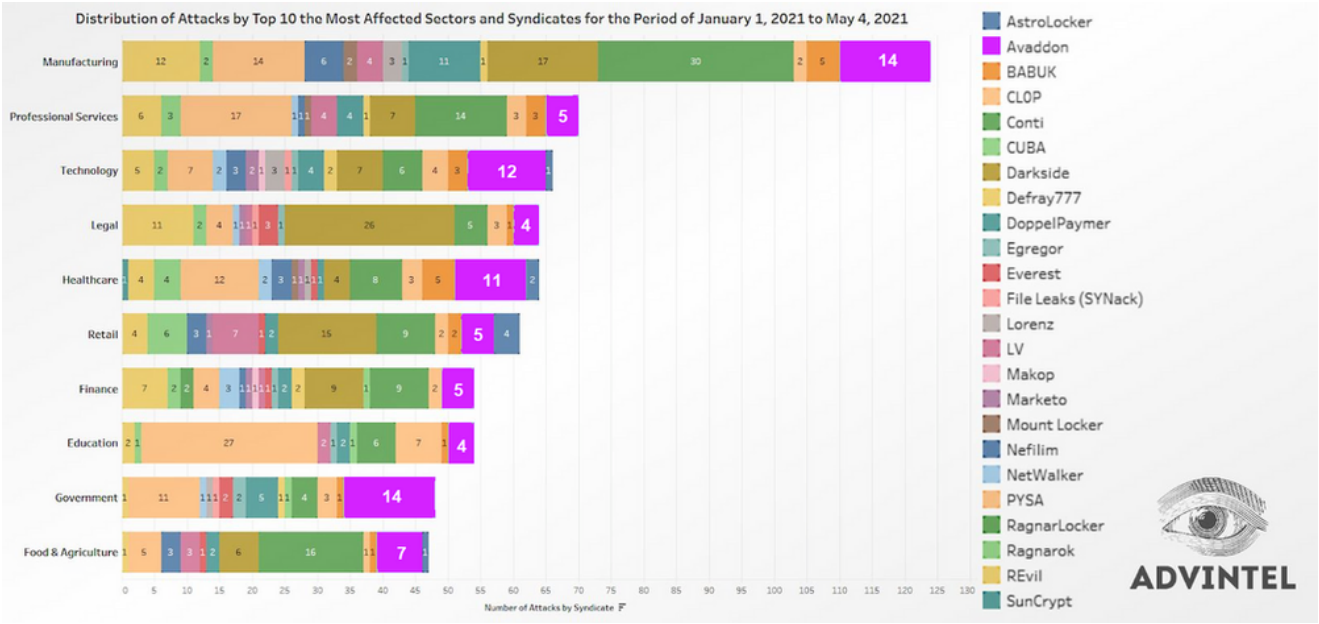
> Avaddon operations targeted companies and governments all across the globe, with the exception of Russia

While investigating the attack first, we discovered **141 unique indicators for RDP compromises** for the victim's domain. This means that Avaddon was using the services of an RDP brute-forcing group. Moreover, two weeks before the attack, a threat actor conveniently published a post on a major underground forum where Avaddon was based, auctioning classified information on the future victim. This access seller happened to be connected to a malware developer specializing in data exfiltration tools. In other words, before Avaddon performed their data-stealing operation, they were able to utilize the entirety of underground services and purchase the full set - RDP access, direct network access, and malware for data exfiltration.

Victimology - Key to Understanding the Adversary

This innovative approach enabled Avaddon to perform several thousand attacks. AdvIntel has analyzed Avaddon's victim's unique datasets to build the most definitive adversarial profile.

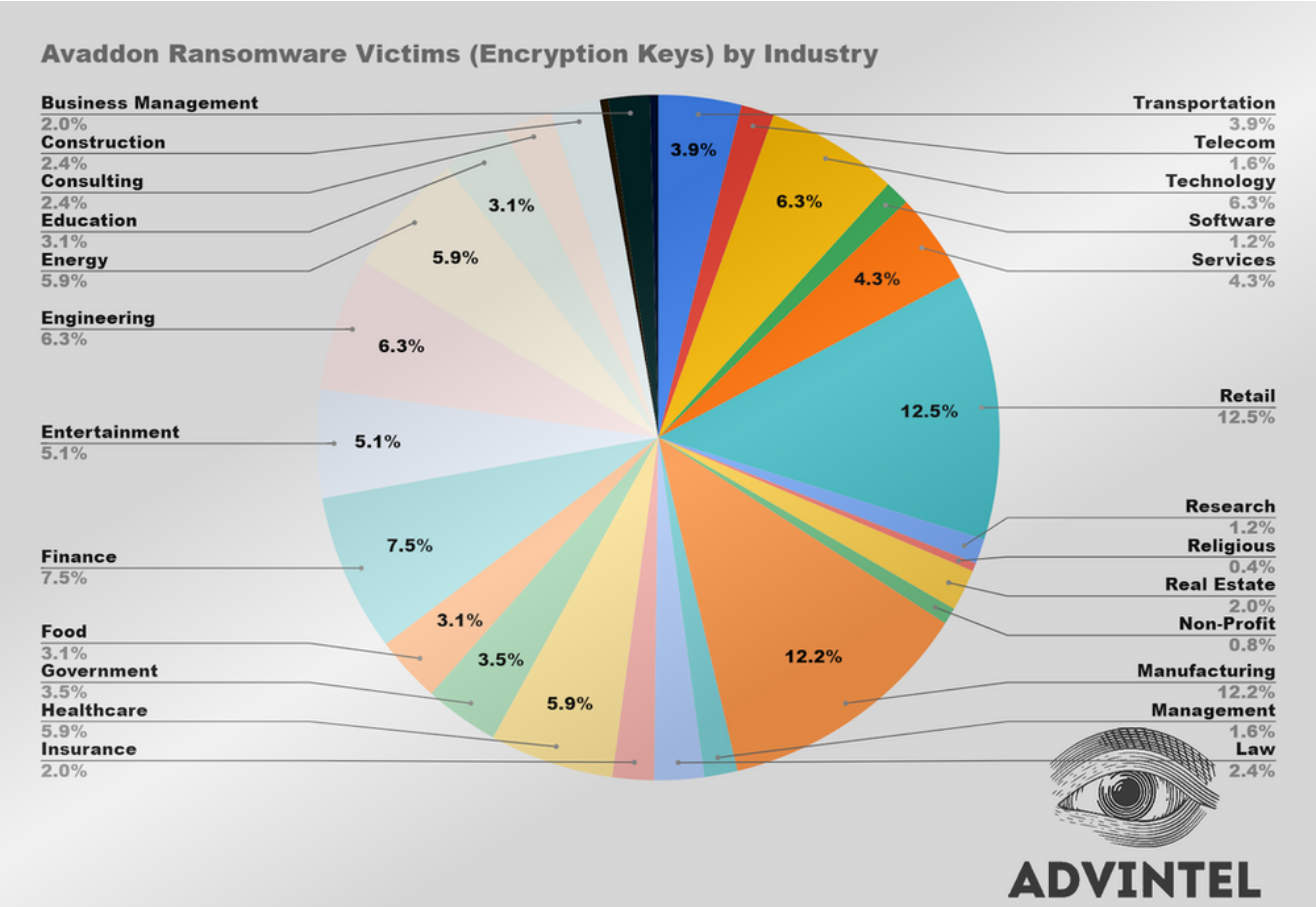
Traditionally, while profiling the group's victimology, companies rely on the data available in public - i.e. ransomware websites. And indeed, even looking at this partial data, which only includes companies whose information was dumped on the shame blogs, we can see that Avaddon played a major role in the threat landscape.



Avaddon ransomware (in bright purple) per industry sector - data based on the publications by Avaddon group on the syndicate's shame blog

However, the victims whose names were published on the shame blog are only the tip of the iceberg. AdvIntel's advanced dataset, **covering all Avaddon victims**, provides further visibility into the gang's operations.

For this statistical research, AdvIntel has selected a special high-value-target dataset. First, we identified the industries which were the primary targets of the group - manufacturing, retail, technology, and engineering being the most preferred sectors most likely because, for the companies in these sectors, even a brief interruption of businesses can imply fatal consequences.



Avaddon ransomware victims defined by the industry of the victims (all-victims dataset)

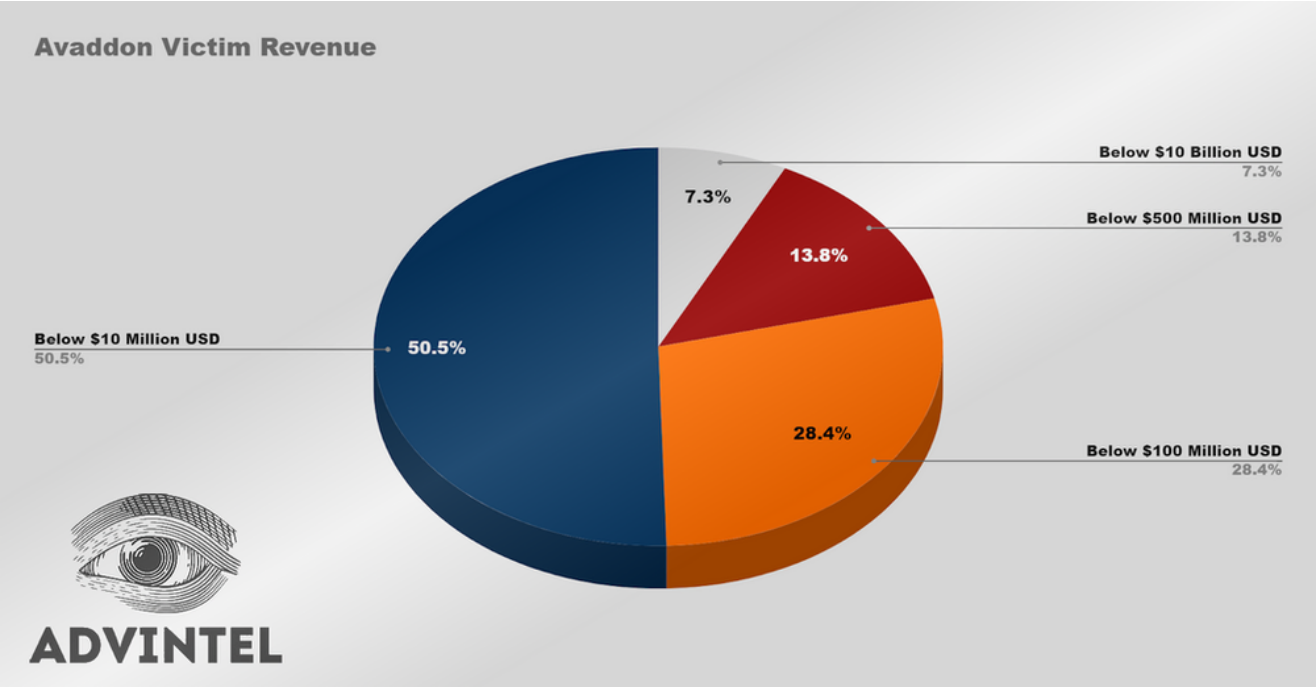
For the next step, we performed market research of the victims' revenue to identify the potential pattern of Avaddon attacks.

The total revenue of all victims was around **$35 Billion USD**. This number is essentially the segment of the market which has been in one way or another threatened by Avaddon malicious operations.

Avaddon's victims can be divided into three categories - small, medium, and large.

The average victim revenue was:

- **$13 Million USD for small businesses**
- **$287 Million USD for medium-sized victims**
- **$3.7 Billion USD for larger businesses**



Avaddon ransomware victims by revenue

Ransonomics: Avaddon Ransomware Profits

Our next research goal was to calculate **how much money the Avaddon group could make before their rapid retirement**. We have utilized our previous knowledge from threat actor engagements to develop realistic formulas of ransom demand calculations supported by the actual Avaddon cases.

Traditionally, all Russian-speaking actors are using the victims' annual revenue to calculate the ransom. After identifying the revenue, they investigate the sector within which the victim operates. The most common calculation which according to our sensitive and credible source intelligence as used by Avaddon was a so-called **"5x5" rule** when 5% of the annual revenue is used to start the negotiations, with annual revenue estimated as one-fifth of the total revenue. In other words, for a victim which has a total revenue of $7 Million USD, the starting ransom price will be $70,000 USD. Typically, Avaddon dropped the price during the bargaining, and the end ransom was around **$50,000 USD** for a successful operation.

However, not all companies out of the two thousand victim list were forced to pay such ransom. In many cases, the negotiation failed or the ransom was minimal - several thousand USD (especially in the very beginning). At the same time, bigger payments were demanded

from larger entities. Here, the “5x5” formula, however, was replaced by a more adequate scale for larger ransom involving 0,01% margins for annual revenue instead of 5%, etc. For a multi-billion dollar company, the demand was constrained by a few million dollars.

> *In other words, in one year of ransomware development, an Avaddon member made the same amount of money as an average Russian would make in a millennium - the best illustration of how lucrative ransomware could be for the region.*

After finalizing all the calculations with a case-by-case study of each victim from the high-value dataset, AdvIntel assessed that the bulk of ransom payments came from over a thousand smaller-sized companies, which were demanded between $30,000 to $70,000 USD and constituted the overall payment of **$55 million** to Avaddon. Over 500 larger businesses in the victim list constituted another **$30 million**, and the rest was divided between smaller payments. As such, our total assessment of Avaddon income is approximately **$87 Million USD**.

Our team has also attempted to calculate the revenue of a core Avaddon team member based on these numbers. Within Avaddon RaaS over 70% of income went to affiliates, therefore, the core team, and especially the leader of Avaddon, received around $26 Million USD. This number was likely divided between at least four individuals, which made the approximate annual income (Avaddon existed for a year) **$7,000,000 USD**. To compare - the median annual income in Russia is estimated at **$7,000 USD**.

In other words, in one year of ransomware development, an Avaddon member made the same amount of money as an average Russian would make in a millennium - the best illustration of how lucrative ransomware could be for the region.

Avaddon Downfall - Black Mark of Cyber Pirates

If Avaddon was so successful, what could have motivated them to quit? The likely answer is fear. The US law enforcement and the Biden administration became very upfront regarding future retaliatory measures against ransomware and the new angle in which ransomware is seen as essentially an act of terrorism. This new take on digital extortion from the world’s leading superpower had a direct response within the underground community - the above-mentioned ransonomics - a carefully and meticulously built web of alliances and supply chains - started to rapidly fail.

Software brokers refused to sell malware to ransomware groups, forums banned RaaS partnerships, and affiliates were left without means and services to disseminate the payload. The cybercrime world was always similar to piracy and it has its own **“black mark” - a deadly stigma sign - after Colonial Pipeline**, ransomware got this sign on itself. Avaddon, which was in the center of the dynamic and turbulent ransomware ecosystem, quickly realized the risks they may face.

When Politics Meets Cybercrime

This realization was likely caused by the recent intervention of politics into the cybercrime domain. Overall, the inner logic of the Russian security landscape presumes that a successful cyber group will at some point become prominent enough to attract the state’s attention. Usually, law enforcement will turn a blind eye to cyber operations unless these operations target Russian citizens or businesses. However, this status quo has changed in May 2021.

After the admin of the largest XSS forum called for a ransomware ban justifying it for political reasons, the community of digital extortionists in Russia was observed to go through stages of paranoia. This was only supported by multiple statements made in the last three months by the Russian government, the Russian Ministry of Foreign Affairs, and by President Putin personally **about establishing an international Russian-American initiative** to establish a joint cybersecurity landscape. The Russian officials likely see this as a tool of de-escalating the US-Russian relationships, especially in the light of the upcoming Biden/Putin summit scheduled for June 16, 2021.

Indeed, the Russian government traditionally goes through rounds of escalation and deescalation with the West. The escalation phase involving military maneuvers in the proximity of the Russia-Ukraine border and in Northern Syria ended in April 2021. Now the Kremlin aiming to address severe challenges of the post-covid economic recession and the turbulent domestic situation is interested in creating a certain framework of stability in the international arena and ensuring stabilized relationships with the US to avoid unnecessary pressure. Cybersecurity - a controversial space or the Russia-US relationship is on the frontlines of this de-escalation agenda.

It is also noteworthy that some of the jurisdictions targeted by Avaddon - Iran, China, and Turkey have strong geopolitical ties with Russia and act as Russian allies or critical economic partners. However, it is unclear if this could have led to any aggravation in the relationship between Avaddon and the Russian state.

> *Usually, Russian security apparatus turns a blind eye to cyber operations unless these operations target Russian citizens or businesses. However, this status quo has changed in May 2021.*

Whatever the true rationale of the Russian politicians calling for international cybersecurity cooperation is, these recent statements have clearly had an impact on the underground cybercrime community. AdvIntel has tracked multiple discussions between top-tier actors working with Avaddon who mentioned that one of the group's affiliates was apprehended by the Russian law enforcement on the eve of the US-Russia summit and that further arrests may follow against the ransomware leaders in order to secure the political landscape.

Avaddon YARA Signature v1:

```
rule crime_win32_ransom_avaddon_1 {
meta:
description = "Detects Avaddon ransomware "
author = "@VK_Intel"
reference = "https://twitter.com/VK_Intel/status/1300944441390370819"
tlp = "white"
date = "2020-09-01"


strings:
        $str0 = "rcid"
        $str1 = "hdd"
        $str2 = "lang"


        $cfg_parser = { 55 8b ec 6a ff 68 74 d8 46 00 64 ?? ?? ?? ?? ?? 50 81 ec 3c
02 00 00 a1 ?? ?? ?? ?? 33 c5 89 ?? ?? 56 57 50 8d ?? ?? 64 ?? ?? ?? ?? ?? 8b f1 89
?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ??
?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7
?? ?? ?? ?? ?? ?? ?? ?? ?? c6 ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? 8d ?? ?? ?? ??
?? 8b ?? 51 8b ce ff ?? ?? 83 ?? ?? ?? ?? ?? ?? 0f ?? ?? ?? ?? ?? 8d ?? ?? ?? ?? ??
8d ?? ?? e8 ?? ?? ?? ?? c6 ?? ?? ?? 8b ?? ?? 85 c0 0f ?? ?? ?? ?? ?? b9 10 00 00 00
c7 ?? ?? ?? ?? ?? ?? 3b c1 c7 ?? ?? ?? ?? ?? ?? c6 ?? ?? ?? 0f 42 c8 83 ?? ?? ?? 8d
?? ?? 0f ?? ?? ?? 51 50 8d ?? ?? e8 ?? ?? ?? ?? c6 ?? ?? ?? 8b ?? ?? c7 ?? ?? ?? ??
?? ?? c7 ?? ?? ?? ?? ?? ?? c6 ?? ?? ?? 83 f8 10 0f ?? ?? ?? ?? ?? 83 c0 f0 b9 20 00
00 00 3b c1 0f 42 c8 83 ?? ?? ?? 8d ?? ?? 0f ?? ?? ?? 51 83 c0 10 8d ?? ?? 50 e8 ??
?? ?? ?? c6 ?? ?? ?? 83 ?? ?? ?? 0f ?? ?? ?? ?? ?? 83 ?? ?? ?? 0f ?? ?? ?? ?? ?? c7
?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ??
?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c6 ?? ?? ?? 8d ?? ??
?? ?? ?? 8b ?? 51 8b ce ff ?? ?? 8b ?? ?? ?? ?? ?? 8d ?? ?? ?? ?? ?? e8 ?? ?? ?? ??
0f ?? ?? ?? ?? ?? ?? 0f ?? ?? ?? ?? ?? ?? f3 ?? ?? ?? ?? ?? ?? ?? 66 ?? ?? ?? ?? ??
?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ??
?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? ??}
        $crypt_imp_seq = { 83 ?? ?? ?? 8b c7 c7 ?? ?? ?? ?? ?? ?? 72 ?? 8b ?? 6a 00
6a 00 8d ?? ?? 51 6a 00 6a 01 6a 00 50 ff ?? ?? ?? ?? ?? 85 c0 74 ?? 56 8b ?? ?? ff
?? ?? ?? ?? ?? 56 6a 00 50 ff ?? ?? ?? ?? ?? 8b f0 85 f6 74 ?? 83 ?? ?? ?? 72 ?? 8b
?? 6a 00 6a 00 8d ?? ?? 50 56 6a 01 6a 00 57 ff ?? ?? ?? ?? ?? 85 c0 74 ?? 8b ?? ??
8d ?? ?? 50 6a 00 6a 00 ff ?? ?? 56 ff ?? ?? ff ?? ?? ?? ?? ??}


condition:
( uint16(0) == 0x5a4d and
( 3 of them )
) or ( all of them )
}
```

Resource:

Avaddon Decryption Tool

https://www.emsisoft.com/ransomware-decryption-tools/avaddon

If you would like to learn more about how AdvIntel helps to make the world ransomware-free, please contact us: info@advintel.tech

Advanced Intelligence is an elite threat prevention firm. We provide our customers with tailored support and access to the proprietary industry-leading "Andariel" Platform to achieve unmatched visibility into botnet breaches and criminal underground and mitigate any existing or emerging threats.