Ransom-War: Russian Extortion Operations as Hybrid Warfare, Part One

nattothoughts.substack.com/p/ransom-war-russian-extortion-operations

Natto Team

Epigraphs:

> *"Hackers are free people. They are like artists. If they are in a good mood, they get up in the morning and begin painting their pictures. Hackers are the same. They wake up in the morning, they read about some developments in international affairs, and if they have a patriotic mindset, then they try to make their own contribution the way they consider right into the fight against those who have bad things to say about Russia." (Russian President Vladimir Putin, June 1, 2017)*

> *"....the government will come and ask us nicely...'Here you go, guys. Now we need you to destroy another country'….we want to destabilize America. You know, destroy it, just as they want to destroy us." (Russian hacker Pavel Sitnikov describes the hacker's ideal world in a 2020 interview, hxxps://expert[.]ru/expert/2020/39/oni-ne-pomnyat-nas-horoshih-pust-ne-zabudut-nas-plohih/)*

> *"Do you have info linking CL0P Ransomware Gang or any other malicious cyber actors targeting U.S. critical infrastructure to a foreign government? Send us a tip. You could be eligible for a reward" (US Department of State Rewards for Justice Program tweet, June 16 2023)*

Previous Natto Thoughts postings have shown how operators of Chinese information security company i-SOON – a group of hackers-turned-IT entrepreneurs – survive in that country's business and political environment: competing with each other for clients, exploits and tools, and always with an eye on the Chinese state, a key patron.

The present series of reports looks at a different set of tech-savvy operators in another authoritarian country: Russian ransomware actors. These are "extortion entrepreneurs," whose stock in trade is bricking up victims' machines and/or threatening to leak private data as a way to extort ransom. Earlier Natto Thoughts postings on the criminal nicknamed "Wazawaka" provided one case study of this group. The present series expands and deepens this analysis, looking more deeply at the social and political context in which Russian cybercriminals operate. It shows that the relationship between Russian ransomware criminals and Russian state agencies is as complex in its own way as is i-SOON's relationship with the Chinese government.

Share

Hybrid Ransomware and Hybrid Warfare

Some ransomware activity appears to be hybrid in two senses—it serves both financial and political motives, and it plays a role in Russia's perceived state of perpetual undeclared "hybrid warfare" against the West.

Hybrid (financial and political) motives for ransomware:

Russian cybercriminal operations sometimes appear to have hybrid motives, serving both the criminals' own financial interests and the political interests of Russian state entities. Well-known examples of Russian cybercriminals undertaking hybrid financial/political operations are Yevgeniy Bogachev, who stole funds from victims' online bank accounts and also spied on Ukraine and the Republic of Georgia; and Alexsey Belan, who stole information from some 500,000 Yahoo user accounts in 2014, sold some of the information to fellow criminals, and shared some of it with a former hacker friend who now worked for Russia's Federal Security Service (FSB). Some Ukrainian cybercriminals, too – both before and after the Russian invasion – are suspected of carrying out espionage or other operations benefiting Russia.

What is hybrid warfare?

These operations are hybrid in another sense as well: they can play a role in Russia's **hybrid warfare** against perceived enemies. Russian media and officials have for many years portrayed Russia as a besieged fortress and depicted the "collective West" as engaged in a constant attempt to demoralize, exploit, and subjugate Russia. They interpret Ukraine's 2014 Revolution of Dignity and its subsequent resistance to Russian aggression as a form of proxy warfare by the West against Russia. They use this idea in an attempt to justify both their kinetic actions against Ukraine and non-kinetic "hybrid" operations against Ukraine's supporters.

Also known as **grey-zone (gray-zone)**, **non-linear, new-generation** or **irregular warfare**, hybrid warfare refers to interstate competition and conflict in circumstances short of declared war. This perceived ongoing twilight struggle includes asymmetric approaches that even countries with relatively weaker military capabilities can undertake. These approaches include cyberattacks and other information operations as well as cultural, political, legal, economic, diplomatic or other nonmilitary approaches (hxxps://cyberleninka[.]ru/article/n/razvitie-i-ispolzovanie-nevoennyh-mer-dlya-ukrepleniya-voennoy-bezopasnosti-rossiyskoy-federatsii) to gain leverage over Russia's adversaries. Russian approaches to hybrid warfare, sometimes called the Gerasimov doctrine, can combine destructive activity in the cyber or physical realm — sometimes disguised as criminal ransomware or idealistic hacktivism — with psychological operations to sow panic, demoralize adversaries, and influence adversaries' decisionmaking.

Russian leaders' sense of being at war with the US and other Western countries, and their "hybrid" strategies for waging this war, show clearly in a classified addendum to Russia's 2023 foreign policy program, seen by the *Washington Post*. The document "calls for an 'offensive information campaign' and other measures spanning 'the military-political, economic and trade and informational psychological spheres' against a 'coalition of unfriendly countries' led by the United States," according to the *Washington Post*'s summary

One advisor consulted during the document's drafting process, Vladimir Zharikhin of Moscow's Institute for the Commonwealth of Independent States, called for Russia to stoke isolationism in America; "enable the destabilization of Latin American countries and the rise to power of extremist forces on the far left and far right there"; support anti-US politicians in Europe; stoke conflict between the US and China over Taiwan; and "escalate the situation in the Middle East around Israel, Iran and Syria to distract the U.S. with the problems of this region," the *Washington Post* wrote.

The Natto Team has pointed to ways in which some of these prescriptions find resonance in real events. For example, the Mideast crisis benefited Russia in many ways. And hacker Wazawaka claims to have unleashed the Conti ransomware that crippled Costa Rica's government in 2022, ostensibly intended "to overthrow the government by means of a cyber attack" and loosen its bonds with the US.

The present Ransom-War series explores the hybrid nature, in both senses, of some Russia-origin ransomware and other cyber extortion. Generally the term "ransomware" refers specifically to malware that encrypts or bricks up victim systems, after which the threat actors demand a ransom in return for a promise to unbrick their systems (although ransomware actors often fail to keep their promises). As the Natto Team has mentioned previously , that bricking stage is often merely the icing on the cake after the threat actors have stolen information. Threat actors can sell the stolen data or threaten to leak it in order to extort more ransom.

Russian Intelligence/Hacker Collaboration: What We Already Know

Multiple excellent reports explore the Russian intelligence services' use of cybercriminals and nonstate actors for political purposes.

Center for European Policy Analysis: Recruitment for Military and Government

In a September 8 2022 report, Russian security experts **Andrei Soldatov and Irina Borogan** comprehensively explored the Russian government's recruitment of cyber talent for the military and government, including from Russian IT businesses.

Recorded Future: Direct, Indirect and Tacit Relationships

A September 9, 2021 report by Recorded Future provides an encyclopedic overview of cybercriminals with known ties to the Russian government. The report distinguishes those Russian cybercriminals who had "direct affiliations" with Russian government agencies from those with "indirect affiliations" and those with "tacit agreements"; Recorded Future defines the latter as the "overlaps in cybercriminal activity, including targeting and timing, that benefit Russian state interests or strategic goals; such activity is conducted without direct or indirect links to the state but is allowed by the Kremlin, which looks the other way when such activity is conducted."

It should be noted, however, that the Recorded Future report extensively cites questionable claims made by Konstantin Kozlovsky, a member of the so-called Lurk group criminal group, who has been in and out of prison since 2016. Every time he came up for a court hearing on the terms of his detention, Kozlovsky would accuse more and more people of being traitors who, he claimed, lured him into criminality for the benefit of foreign intelligence services. The stories appear to be intended to tell what his listeners wanted to hear in order to get a lighter sentence. (This did not help him; in February 2022 he received a 14-year sentence). The Recorded Future report and other media reports point out some of his claims that appear false or illogical, but they and other reputable commentators seem to view his claims as having a grain of truth. It is unclear which, if any, of Kozlovsky's claims are credible.

In a January 2023 followup report, Recorded Future finds that after Russia's full-scale invasion of Ukraine in February 2022, "cybercriminal threat groups continue to occupy important roles — in direct, indirect, and tacit capacities — with the Russian government. For cybercrime groups who have pledged their allegiance to the Kremlin, the unspoken connections have deepened. Russian cybercriminals and self-described hacktivists are actively involved in operations targeting Ukrainian entities and infrastructure, as well as entities located in states that have declared their support for Ukraine."

Atlantic Council: "Spies, proxies, and spectrums of Russian cyber behavior"

One particularly valuable synthesis and discussion of what we know about state-nonstate cyber collaboration is "Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior," a September 19, 2022 report by Justin Sherman for the Atlantic Council, a US think tank. This report explores in depth how the Russian government "actively cultivates" cybercriminals as one part of "a complex web of Russian cyber actors" and "continues to leverage this ecosystem for purposes that extend beyond criminal activity such as operations for Russian intelligence services."

Sherman explains, "Putin does not control all these groups, and even if the FSB does engage with a hacker on a local level, Putin is (by and large) not involved in the day-to-day minutiae…" In reality, Sherman says, "There are degrees of Russian government involvement with most Russian cyber actors, whether it is through active financing, tacit approval, or another kind of engagement entirely. It is also possible that some activity is

entrepreneurial by design, with nonstate hackers and developers auditioning their capabilities to capture the attention of the state" in an atmosphere of "Darwinian entrepreneurialism." (This resembles the cutthroat business environment in which the Chinese company i-SOON operates).

Sherman enumerates the benefits that collaboration with cybercriminals and other nonstate cyber actors brings to the Russian government. In addition to the cash these cyber actors bring into the country, benefits include the ability to wage "hybrid" warfare deniably below the level of armed conflict, and the ability of the government to tap skilled personnel who finance themselves and bear the risks of their own operations.

At the same time, these actors often squabble with each other (as we saw in our report "Wazawaka & Co.") and can be unpredictable, potentially carrying out operations that will backfire on the government. Indeed, as Natto Thoughts research and an April 2024 Mandiant report have shown when state cyber actors work with ostensibly hacktivist personas such as Solntsepek, it is not always clear to what degree the handlers in the Russian intelligence services have control over them.

The exact mechanism by which Russian intelligence services suggest targets to cybercriminals needs further elucidation, Sherman wrote. The present Natto Thoughts series addresses that question, with a particular focus on the subset of cybercriminals who focus on ransomware.

Ransomware Actors and the Russian State: What We Know

Natto Thoughts has previously profiled threat actors nicknamed Solntsepek and Wazawaka as examples of cybercriminals whose targeting and timing aligned with Russian strategic priorities on at least some occasions. In the case of Wazawaka, we mentioned several types of evidence suggesting some kind of coordination between Wazawaka's criminal circle and Russian security services. This evidence includes Wazawaka's timing and political commentary in the attacks on Costa Rica and the Washington DC Metropolitan Police Department; and the DarkSide and AlphV groups' attacks on Colonial Pipeline and other critical infrastructure. We noted that after Putin disingenuously compared Russian hackers to independent-minded artists, Wazawaka appears to have embraced that ironic image by identifying himself in his Twitter bio as a "Russian security artist." Wazawaka and these other cybercriminals appear in some cases to have been acting not as purely rational businesses selecting the most lucrative targets. Rather they are steeped in a political atmosphere portraying all Russian citizens as at war with the West, and in some cases they have proven links with Russian intelligence services.

As the Natto Team has pointed out, these relationships are subtle and likely indirect. Natto Thoughts' first post, "Putin: Spy as Hero," compared Russian influence operations to throwing spaghetti at the wall to see what will stick: Putin's speeches and state media set the

tone and identify targets, and Putin loyalists compete to attack those targets, allowing Putin to deny direct involvement. The Russian leadership's reliance on "entrepreneurs of influence" yields what security analyst Mark Galeotti has dubbed an "adhocracy" of "competing, semi-autonomous actors expected to …generate their own plans to work toward the state's broad objectives." A previous Natto Thoughts post cited cyber law researcher Jason Healey's attempt to categorize variations on the hacker/state relationship via a 10-point "spectrum of state responsibility" for cyber threat operations, ranging from "state-prohibited" to "state-encouraged" to "state-integrated" operations.

The Natto Team has also analyzed the 2023 campaign by an affiliate of the Clop (a.k.a. Cl0p) ransomware gang to breach hundreds of entities with a supply chain attack exploiting flaws in the MOVEit file sharing tool. That analysis pointed to some targeting of national security-sensitive entities, suggesting the Russia-origin Clop actors may have been performing espionage that could benefit a Russian state entity. (A supply chain attack is an attack on an entity that provides software or other products or services to multiple clients; by breaching the supplier's system, the threat actor can steal information from, or taint the product supplied to, multiple clients at once. Examples of supply chain attacks are the Solar Winds espionage operation discovered in 2020 and the Petya.A/NotPetya attack on Ukraine in 2017).

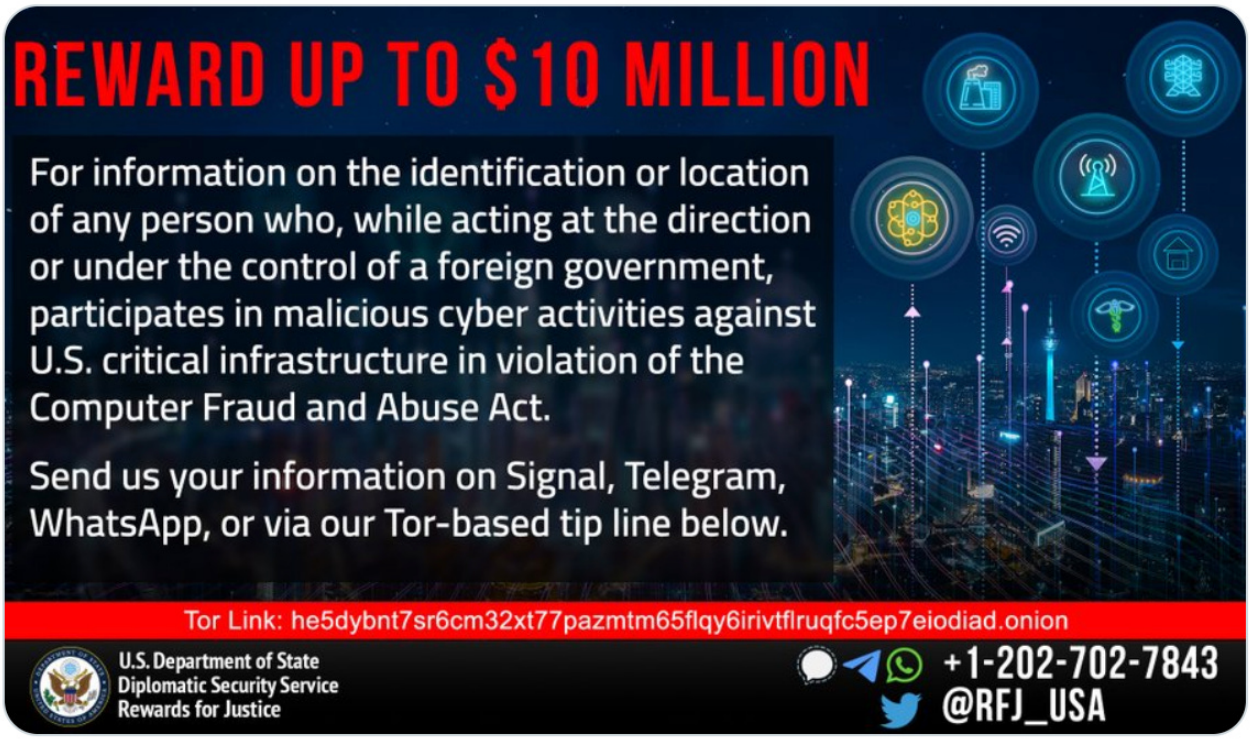
US Considers Possible State Ties of Cl0p and Other Ransomware Groups

The US government appears to share the Natto Team's suspicion that the Clop group, or other ransomware operators, may be working for Russian security services. On June 16 2023 the US State Department's Rewards for Justice program tweeted, "Do you have info linking CL0P Ransomware Gang or any other malicious cyber actors targeting U.S. critical infrastructure to a foreign government? Send us a tip. You could be eligible for a reward." The tweet reproduced a poster announcing a bounty of up to $10 million for "info linking CL0P Ransomware Gang or any other malicious cyber actors targeting U.S. critical infrastructure to a foreign government."

Do you have info linking CL0P Ransomware Gang or any other malicious cyber actors targeting U.S. critical infrastructure to a foreign government?

Send us a tip. You could be eligible for a reward.

#StopRansomware



12:15 PM · Jun 16, 2023 · **412.7K** Views

June 16 2023 tweet by the US Department of State's Rewards for Justice Program

US and UK Identify Ransomware Groups Working with the Russian State

On several occasions, the United States and United Kingdom governments have explicitly stated that certain Russian ransomware-related cybercriminals have cooperated in some way with Russian intelligence services.

- On December 5 2019, The US Treasury Department – relying partly on intelligence provided by the UK's National Crime Agency -- sanctioned the **Evil Corp** group and its leader, **Maksim Yakubets**, for working for the Russian Federal Security Service (FSB). Independent researchers also discovered that Yakubets is married to the daughter of a high-level FSB retiree. Another Evil Corp member, **Igor Turashev**, was a winner in a 2023 hackathon associated with the mercenary and information warrior Yevgeniy Prigozhin's Wagner Group.

- On August 11 2022 the US State Departments' Rewards for Justice program offered a reward of up to $10 million for information "that ties hacking groups such as **Conti, TrickBot, Wizard Spider**....or any malware or ransomware to a foreign government targeting U.S. critical infrastructure, you may be eligible for a reward."

- By February 9 2023 the US and UK announced sanctions against 7 members of the Trickbot and related Conti groups and added 11 more individuals to sanctions lists on September 7 2023. In the February UK announcement, the National Cyber Security Centre assessed that the Conti group's "targeting of certain organisations, such as the International Olympic Committee… almost certainly aligns with Russian state objectives," and that Conti actors "likely have extensive links to other cyber criminals, notably EvilCorp and those responsible for Ryuk ransomware." The US announcement from September read, "Members of the Trickbot group are associated with Russian intelligence services. The Trickbot group's preparations in 2020 aligned them to Russian state objectives and actions taken by the Russian intelligence services. This included targeting the U.S. Government and U.S. companies."

- In a February 22 2023 interview, Andrew Boyd, former director of the Center for Cyber Intelligence at the US Central Intelligence Agency (CIA), said the CIA tracks ransomware groups and "where those ransomware actors meet state actors" (minute 31:13 of the interview). He said, "Frequently the nexus between the non-nation state actors, ransomware actors and criminal enterprises are a dotted line relationship connected to our nation state adversaries…" When asked about the US and UK statements on Trickbot members' association with Russian intelligence services, Boyd said some Russian criminals have connections with the FSB or with the GRU (Russia's military intelligence), although not in the sense of a client-employer relationship (minute 34:50). Rather, the criminals are "on call to do certain activities" in return for state tolerance of their other activities.

Other researchers acknowledge use of ransomware in nation-state offensive operations, but vary in their assessment of its extent

"I, 100 per cent, believe they're being leveraged by the Russian government," cyber analyst Jon DiMaggio told ABC Australia in 2023, referring to the REvil ransomware group's support of Russia's war against Ukraine. "They're helping the FSB or the GRU … creating malware

and facilitating attacks against Ukraine to better the mission of Russia."

Check Point: Timeline and Overview

Israel-based cybersecurity company Check Point provides an extensive timeline and helpful overview of major events in the history of ransomware. But Check Point says Iran was the first country to use ransomware in nation-state offensive operations, starting in September 2020. It says Russia began to use ransomware as a tool in nation-state operations only in February 2022. That is debatable. Natto Thoughts assesses with medium confidence that the Russian state has likely been at least tacitly encouraging ransomware operators to target Russia's adversaries since at least 2018. The Natto Team will discuss this in a future posting.

Stanford Internet Project Study: Political Targeting and Timing

Stanford Internet Project researchers trace politically motivated Russian ransomware operations back to at least 2019. In a July 2023 study they wrote about an incident occurring that year in the US state of Louisiana:

> Hours after polls closed in Louisiana's 2019 gubernatorial election, a ransomware attack brought down 10% of the state's computer servers and prompted the governor to declare a state of emergency...This attack followed a seemingly unrelated one, in which a breach of a Louisiana state contractor allowed attackers to access servers across the state; although the attackers had gained access to these servers months earlier, they waited until six days before the election to launch a ransomware attack.

The Stanford researchers note, "Although neither attack prevented the state from tallying votes or certifying results, they highlight that ransomware, which is often considered an apolitical crime, may also have political motivations."

To test their assessment, the Stanford researchers analyzed the timing of double extortion [ransomware and data theft] attacks posted on ransomware operations' dark-web sites between November 2021 and April 2022, along with another dataset from cybersecurity firm Dark Tracer spanning the period May 1 2019 to July 23 2021. The researchers found that the threat actors' choice of targets and timing aligned with politics, identifying "trends in the targeting of these attacks that are unlikely to be explained by financial motivations alone":

> First, we find an increase in the number of attacks by Russia-based ransomware groups before elections in several major democracies, with no similar increase in attacks by other groups. This suggests that Russia-based ransomware groups may increase attacks before elections as part of state-backed efforts aimed at election meddling.
>
> Second, we find a decrease in the number of daily ransomware attacks after Russia's invasion of Ukraine, which we argue is likely driven by Russia's recruitment of ransomware operators to aid its cyber offensive against Ukraine.
>
> Third, we find that companies that withdrew from or suspended operations in Russia after the invasion were more likely to experience a ransomware attack in the months after the invasion; this suggests that ransomware groups may have retaliated against these companies (as these actions were widely perceived as a condemnation of the invasion).

Note: the Stanford researchers make a few stumbles that show they are not steeped in the world of Russian cybercrime. For example, they write that some Eastern European languages are dialects of the Russian language. They also incorrectly say EvilCorp developed the REvil malware, but they neglect to say that EvilCorp did develop BitPaymer and WastedLocker malware . (Good reference sources on these groups include Malpedia and a Thailand-based Threat Actor Encyclopedia). Nevertheless, the Stanford Researchers' main point in this exercise was to identify groups that are Russian, and there they are relatively accurate, so their argument holds.

The Stanford researchers point out how the election-era hacks could have multiple motives. One of these could be to "create a perception hack, in which news of a cyber intrusion leads the public to question the reliability of election results regardless of the attack's actual impact." They referred to Russians attempting that kind of "perception hack" against Ukraine's 2014 presidential election, which the Natto Team previously discussed here. Another psychological operation would be to "create chaos in democracies during a politically sensitive time," as Russia-backed hackers attempted to do against Estonia and the Georgian Republic in 2007-2008.

The Stanford researchers also probed contacts between the infamous Conti group and the Russian government, based on the February 2022 leaks of the group's internal communications. (In-depth reports based on the Conti and related TrickBot leaks include those by Check Point, Brian Krebs, and Nisos, and the Global Initiative on Transnational Organized Crime provides a comprehensive bibliography on the group). The Stanford researchers conclude that "the Kremlin maintains decentralized yet cooperative relations with ransomware groups," providing immunity from prosecution in return for "plausible deniability

for state-backed cyber operations as well as access to specialized skills." As an example of the latter, they say, "tools from Conti and another Russia-based ransomware group, Cuba, have been re-purposed to aid the Russian government's cyber offensive against Ukraine."

Trellix Report on Conti Group: The Value of Original-Language Screenshots:

A report by Trellix, analyzing the leaked Conti chats, has the advantage of providing the dates and the Russian originals of selected messages. It helpfully pulls together abundant evidence of Conti members' ties with Russian government agencies. In addition, the Russian-language screenshots show additional nuance and sometimes significant revelations that those who rely on machine translations can miss. The Natto Thoughts posting "Too Many Toads" provides insights that enrich the Trellix findings. Evidence of Conti's ties with Russian intelligence includes the following:

- Group members suspected that Conti group leader "Stern" had ties with the FSB or other agencies and was "in service to Pu," referring to Russian President Vladimir Putin, and that these connections helped Conti escape the Russian law enforcement crackdown of late 2021 and early 2022.
- Conti member "Target," who acted as a government liaison, appeared to indicate that the group received some assignments from the Saint Petersburg branch of the FSB.
- Conti group member "Professor" said he was receiving payments from a contact who worked in foreign intelligence (по внешке), presumably Russia's SVR. This appeared to include providing lists — likely of compromised computer systems — to the SVR hacker team Cozy Bears (a.k.a. APT29).
- In addition to paid work, Conti leader Stern feels the need to do unpaid volunteer work for the Russian state, just as Soviet-era Young Pioneers, a Scout-like organization, did volunteer work.
- As of 2020, Conti members took care not to accidentally harm anyone in Russia, a key condition for avoiding arrest. They also appeared to have been told to avoid Chinese targets as well, in alignment with Russian strategic interests at the time.
- Conti group members worked with the Maze ransomware group to breach systems at US military contractor Academi (formerly Blackwater) and other military targets.

Kela: Focus on the Conti Group's Team "For Government Topics":

Several researchers picked up on the fact that Conti member "Target" wanted to set up a special team "for government topics" (таргет там собрался отдельный офис делать у себя под гос темы). This appeared in a July 20, 2020 chat discussing a recent operation by Conti and Maze group members to breach systems at US military contractor Academi (formerly

Blackwater) and other military targets. The phrase “for government topics” could be understood two ways: 1) as a liaison office for relations with Russian government agencies or on operations of interest to the Russian government, or 2) as an office dedicated to targeting foreign governments. Israel-based cybersecurity firm Kela interprets it as targeting foreign governments, although the two meanings are not incompatible. Kela summarizes additional comments by Target about how such a “government topics” team would work; a future Natto Thoughts posting will address this further.

This Natto Thoughts Series Explores The Relationship Between Russian Intelligence and Ransomware Actors

If some ransomware operators are taking cues from Russian intelligence services in their targeting and timing, how does this take place? In recent years, investigations, indictments, and the words of the criminals themselves have fleshed out that picture. This Natto Thoughts report provides more granularity about the relationship between cybercriminals and the Russian state, focusing in particular on ransomware actors.

This series of postings will address the following:

- What cybercriminals say about this relationship, finding that they portray themselves as both entrepreneurs and warriors for the Russian motherland, but that their patriotic duty sometimes conflicts with profit-making;
- What Russian government statements and actions, from at least as early as 2016, show about attitudes toward using ransomware actors and other cybercriminals in hybrid conflict to undermine enemy countries;
- What we know about how Russian officials co-opt ordinary criminals for political missions;
- What we know and can hypothesize about mechanisms of communication and coordination between Russian security services and cybercriminals, particularly ransomware criminals;
- How this understanding applies to famous ransomware incidents. In examples of ransomware incidents whose targeting and timing appear consistent with political motivation, we consider whether these represented coordination with state actors.

Thanks for reading Natto Thoughts! Subscribe for free to receive new posts and support the Natto Team’s work.