

The Dark Web of Intrigue: How REvil Used the Underground Ecosystem to Form an Extortion Cartel

advanced-intel.com/post/the-dark-web-of-intrigue-how-revil-used-the-underground-ecosystem-to-form-an-extortion-cartel

AdvIntel

July 10, 2020



BY YELISEY BOGUSLAVSKIY
& DANIEL FREY



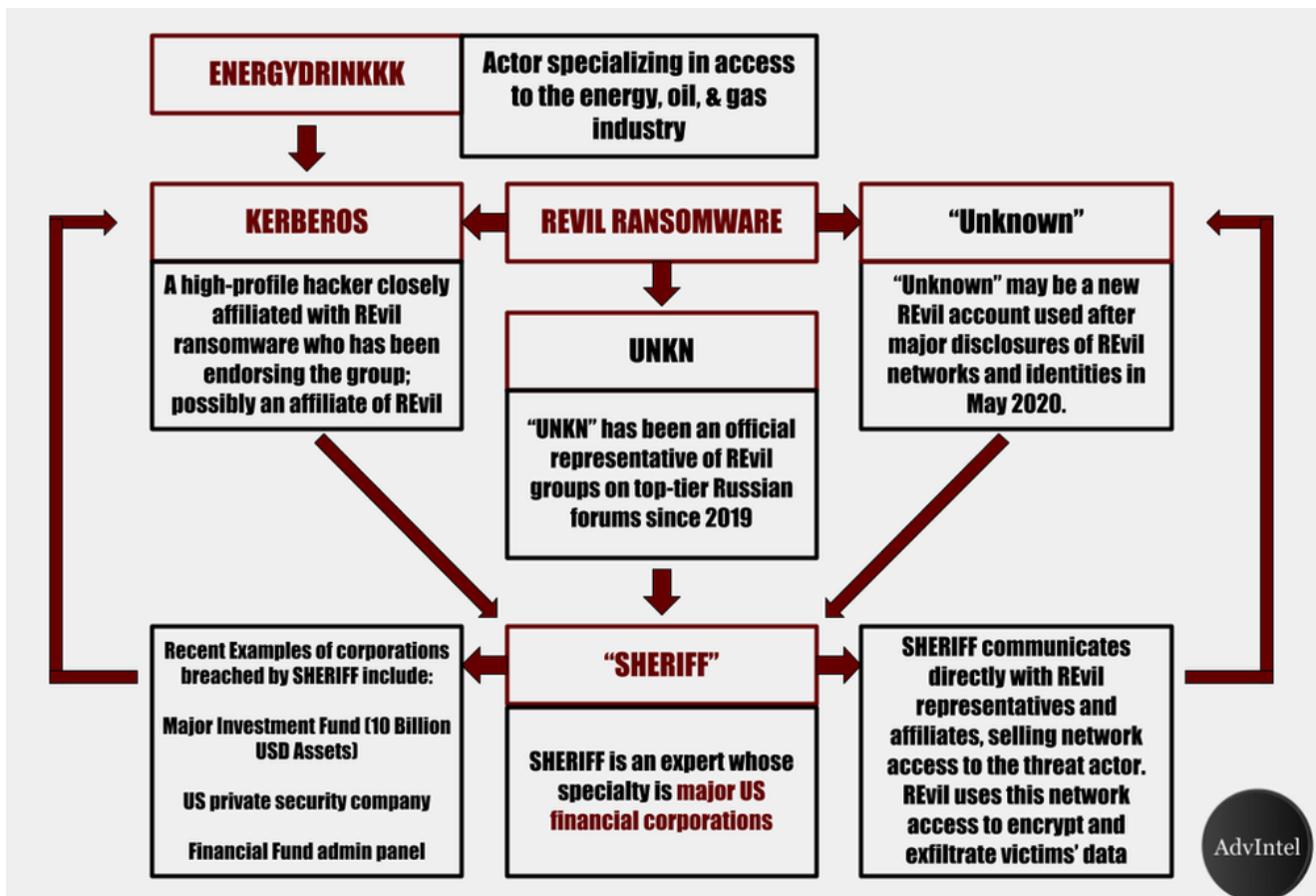
The group's activities on top-tier DarkWeb forums also provide a unique insight into the current workings of the ransomware ecosystem.



- o Jul 10, 2020
- o
- o 8 min read

Key Takeaways:

- Just about one year ago, the makers of the infamous GandCrab ransomware announced their retirement, having reportedly earned an astonishing \$2 billion since their entry into the ransomware market in January 2018. The vacuum was quickly filled, however. Forensic and malware evidence was soon discovered connecting GandCrab’s malware to a new ransomware variant which was about to wreak havoc on a global scale: REvil.
- REvil’s recent activities in the cybercriminal underground significantly alter the ransomware threat landscape. Its interactions with high-profile threat actors suggest a preference to work as part of a network intrusion-focused criminal syndicate, which is an entirely novel business model to a Russian-speaking ransomware community historically reliant on mass spearphishing.
- In this way, REvil and the actors it interacts with form a cohesive, underground economy, in which victims – and the data they own – are the main commodity.
- Given REvil’s targets’ prominence and large revenue streams, it appears that REvil is now aiming for high-profile, high-reward attacks in critical industries.
- Advanced Intelligence provides possible mitigations and network defense measures that can be taken to disrupt REvil and their affiliate attacks.



Background

Just about one year ago, the makers of the infamous GandCrab ransomware announced their retirement, having reportedly earned an astonishing \$2 billion since their entry into the ransomware market in January 2018. The vacuum was quickly filled, however. Forensic and malware evidence was soon discovered connecting GandCrab's malware to a new ransomware variant which was about to wreak havoc on a global scale: REvil.

REvil's rise was rapid. It has victimized enterprises and municipal governments alike, having claimed 12.5% of the ransomware market share as of Q2 2019. By mid-May of this year, the threat actor behind REvil announced that it had infiltrated a major entertainment law firm's computer systems, and threatened to release information on U.S. President Donald Trump if they did not receive a \$42 million ransom. In this way, the REvil ransomware gang - now reportedly considered a terrorist organization by the FBI - has become more than just a hacking collective. REvil now dominates the threat ecosystem as the ultimate extortionist cartel.

The recently reported attack against Grubman Shire Meiselas & Sacks was merely the latest in a series of high-profile ransomware incidents perpetrated by the group. In early June, for instance, REvil attempted to auction off data from Agromart Group, a Canadian agricultural company; in mid-May, it was announced that REvil had attacked Sherwood Food Distributors, a food distribution company based in Detroit. Notably, REvil (as well as some other ransomware groups, such as Ragnarok) has proven particularly receptive to Citrix and remote desktop protocol (RDP) exploits, a tool, technique, and procedure (TTP) we will delve into later in this report. For REvil to have reached its level of notoriety and impact, however, it required more than just technical talent. Fortunately for REvil and unfortunately for their victims, the collective adopted a practice from their predecessor, GandCrab - reliance on decentralized criminal networks.

In our previous reports, we observed how the GandCrab group revolutionized ransomware, leveraging major criminal networks to conduct its activities. REvil has followed the same path. Their representative(s), known across the DarkWeb by the alias "UNKN", does not act alone: they partner with other threat actors to bolster their own capabilities.

Force Multiplier “Sheriff”: An Expert In the Financial Sector & Citrix Breaches

REvil has been explicitly interested in recruiting top talent on the DarkWeb since Fall 2019. Specifically, they were endorsed and supported by a hacker who uses the alias “Kerberos”; we delve into “Kerberos” and their activities later in this report. “Kerberos” is a breach specialist and REvil’s connection with the actor fits into a late-2019 trend, in which ransomware groups and breach specialists collaborated in an effort to maximize profits.

Recently, REvil has deepened their cooperation with members of the criminal underground, recruiting specialized experts as force-multipliers for their enterprise. One of their main accomplices operates under the alias “Sheriff”; they are a rising star of the Russian-speaking underground and specialize in attacks against banks, financial institutions, and government agencies.

Sheriff’s main TTPs center on the use of brute-forcing (a method that relies on software to guess many passwords, in the hopes of gaining access to an account) and credential-stealing malware. Historically, “Sheriff” has navigated compromised networks and admin panels and then exfiltrated data using SQL injections (a web-based attack reliant on nefarious code written in the SQL database querying language) and cross-site scripting (XSS) (an attack that targets victims’ web browsers). In their interactions with REvil, however, “Sheriff” has likely limited their activity to selling access to victims’ networks; REvil likely uses this access to perform the actual data encryption and exfiltration.

In the past, Sheriff’s targets have included a major investment fund (\$10 billion in assets) and a private U.S. security company. Over the last couple of weeks, they have actively exploited the Citrix remote desktop protocol (RDP), and advertised access to a number of high-profile/high-revenue entities, including several universities in Australia, Canada, and the United States; companies focused on security, long-distance passenger transportation, warehouse materials, and cloud computing; and a “famous” European capital and cities in Spain and France.

Earlier in June, “Sheriff” boasted Citrix RDP access to a European construction company focused on oil projects, as well as access to 3,200 Cpanel accounts. Moreover, in May, “Sheriff” advertised administrative access to an e-commerce entity’s WordPress plugin, as

well as access to approximately 815,000 orders, and information on “signatures, discounts, bonuses,” and “gifts”. Most recently, on July 6, 2020, “Sheriff” offered access to 62,000 eToro accounts.

As mentioned previously, “Sheriff” often pursues Citrix credentials to gain access to victims’ networks. RDP, when used for non-illicit means, can serve as a useful way for information technology (IT) teams to access computer systems and diagnose problems. When used nefariously, however, RDP can allow unauthorized users to claim administrative control over a victim’s computer system or associated network. There have been numerous instances – particularly in recent months – in which nefarious actors have taken advantage of Citrix exploits.

In January 2020, for example, it was reported that the Ragnarok ransomware group had taken advantage of one such exploit, leading to attacks on dozens of FireEye customers. There have also been recorded instances of REvil using Citrix exploits in ransomware attacks, such as one against “German car parts manufacturer Gedia Automotive Group”. Considering “Sheriff” and REvil’s interaction in May 2020 (see below), “Sheriff’s” focus on Citrix exploits, and REvil’s previous use of such exploits, we assess that REvil is likely to use Citrix exploits again in future attacks.

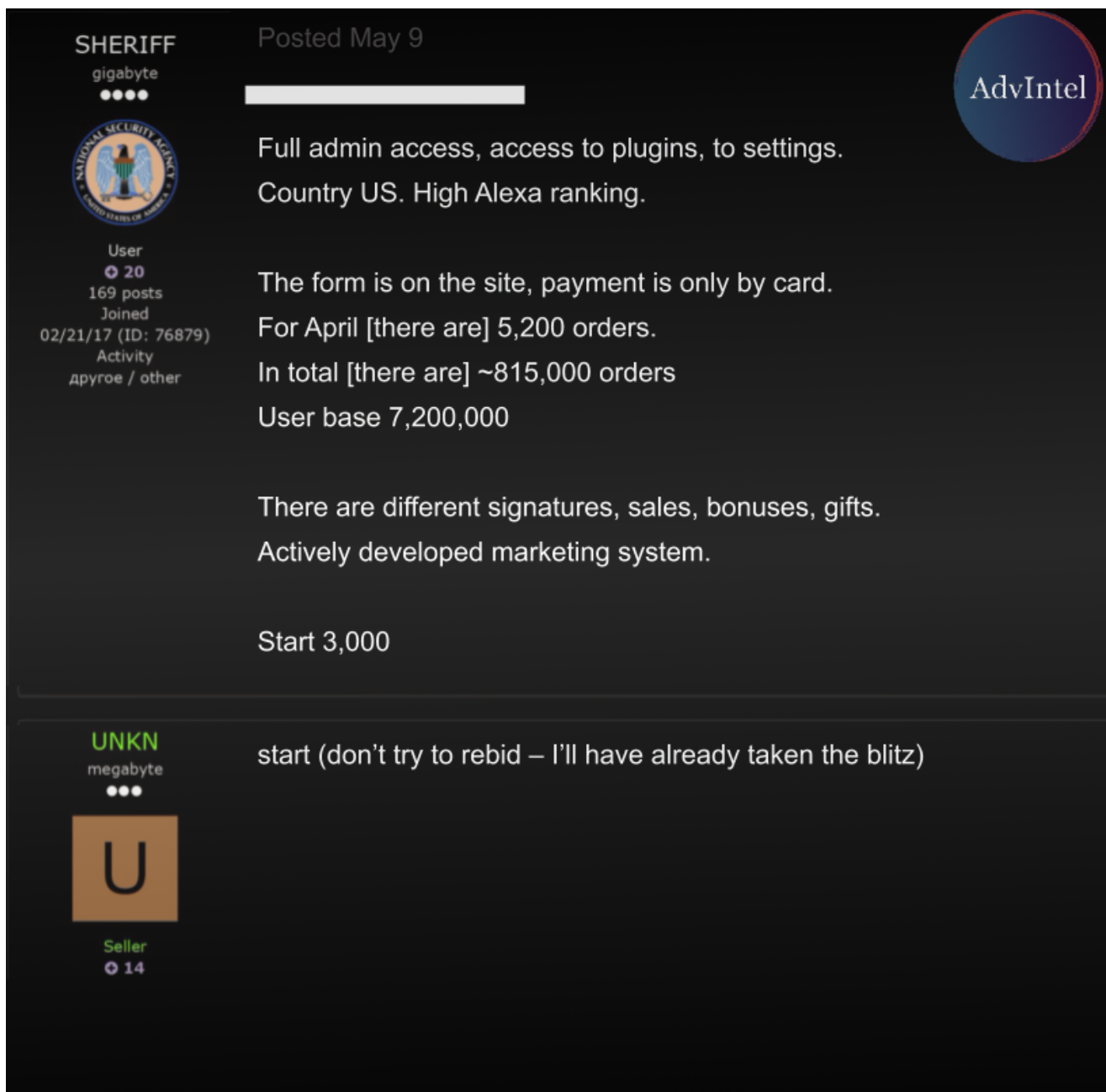


Image 1. UNKN, the head of REvil enters in an underground auction to purchase SHERIFF's with paying the Blitz (a price significantly higher than the initial bid price) and advice the other auction participates to not attempt to compete with them on this bid

“Sherrif’s” interactions with REvil, however, likely go beyond the group’s “UNKN” alias. REvil has also likely contacted “Sheriff” under the name, “unknown”. “UNKN’s” increasing notoriety led to the deletion of REvil’s threats against President Trump on major DarkWeb forums. REvil may be using the “unknown” alias as a new identity in the wake of their “unmasking”.

We have identified this new alias in communications with "Sheriff". Assuming "unknown" is a new alias for REvil, "Sheriff's" interactions with "unknown" are notable, given both threat actors' notoriety and previous activity in the cybercriminal underground.

 <p>SHERIFF гигабайт ●●●●</p> <p>Пользователь ● 20</p>	<p>Posted May 18</p> <p>We will sell [redacted] account Balance \$160 For the entire duration there were \$18k of transactions One active company is abandoned, 2 are on pause Price \$450</p>	
 <p>[redacted] петабайт ●●●●●●</p> <p>Пользователь ● 21</p>	<p>Posted May 18</p> <p>Atslover write he'll take it</p>	
 <p>unknown байт ●</p> <p>Пользователь ● 0</p>	<p>Posted May 18</p> <p>I'll take it</p>	
 <p>SHERIFF гигабайт ●●●●</p> <p>Пользователь ● 20 171 публикации</p>	<p>Posted May 18</p> <p>Sold. 50 accounts in stock, without balances with history ready to use</p>	

Image 2: SHERIFF communicates with a possible alternative alias of REvil in order to process a high-profile access

“Sheriff” is a high-profile threat actor focused on Citrix; their interactions with REvil amplify the ransomware group’s threat to entities employing this kind of software, which is ubiquitous and widely used. Users of Citrix with RDP must remain wary of the software’s vulnerabilities, be prepared to patch them when available and monitor and review network perimeters for any externally-exposed RDP servers.

Force Multiplier “energydrinkkk”: Expert In Attacks Against the Energy Sector

REvil has also proven closely affiliated with “Kerberos”, a high-profile threat actor who has endorsed REvil directly. “Kerberos” is active on the top-tier Russian-language forum, posting ads for coders and solicitations for access to various firms’ networks/financial information. Notably, “Kerberos” victim list includes a hospital, which follows a worrisome trend: healthcare organizations have seen an uptick in attacks amidst the COVID-19 crisis.

Moreover, “Kerberos”, likely an affiliate of REvil, has interacted with “energydrinkkk”, an underground threat actor who targets companies in the energy industry. “Energydrinkkk” recently posted a solicitation offering RDP access to a United Arab Emirates/Canada-based energy company’s Microsoft Online workspace. “Energydrinkkk’s” RDWeb exploit allegedly provides access to a company engineer’s workspace on Microsoft Online, which houses internal communications, as well as information on company contracts and purchases. “Energydrinkkk” also claimed to be able to access company email, accessible through employees’ personal computers. “Energydrinkkk” also alleges to have copied passwords and approximately 400 pieces of contact information (including postal addresses, names, and telephone numbers).

On May 8th, “Energydrinkkk” expressed a desire to enable a ransomware attack against the company, and “Kerberos” – again, a likely affiliate of REvil – has subsequently responded in kind; “Kerberos” posted on May 20th that they were interested in buying “Energydrinkkk’s” access for \$1,500.





	<p>Posted June 10</p> <p>Citrix universities RDP access</p> <ol style="list-style-type: none"> 1. 2RDP Revenue: \$650 Million Australia 2. RDP university Canada 3. 2RDP Revenue: \$2 Billion US 4. RDP Revenue: \$116 Million US 5. 7RDP Revenue:\$1 Billion Australia 	
	<p>Start 5000</p> <p>Step 1000</p> <p>End of auction 24 hours after the last bid.</p> <p>All questions can be clarified via pm [private message]</p>	
	<p>Posted June 10</p> <p>Companies Citrix RDP access</p> <p>RDP Revenue: \$21 Million security company honey</p> <p>2RDP: company providing long-distance passenger transportation</p> <p>RDP Revenue:\$287 Million US company supplier of warehouse materials</p>	
	<p>Start 3500</p> <p>Step 500</p> <p>End of auction 24 hours after the last bid.</p> <p>All questions can be clarified via pm [private message].</p>	
	<p>Posted June 10</p> <p>Citrix access city administrations</p> <ol style="list-style-type: none"> 1. Spanish City. citrix RDP 2. French City. citrix RDP 3. City in Europe, well-known to all, a capital. Citrix RDP 	
	<p>Start 7000</p> <p>Step 1000</p> <p>End of auction 24 hours after the last bid.</p> <p>All questions can be clarified via pm [private message].</p>	

Image 3: SHERIFF is one of the leading hackers in the Russian-speaking community specializing on RDP and Citrix

Both “Kerberos” and “Sheriff” have expressed interest in RDP exploits. “Kerberos”, likely acting on behalf of REvil, has attempted to purchase such exploits; “Sheriff”, meanwhile, has sold such exploits to REvil. Given the fact that both “Sheriff” and “Kerberos” maintain interest in RDP attacks – particularly those targeting energy-focused companies – and considering that both threat actors have recently interacted with known/likely representatives of REvil ransomware, AdvIntel assesses that REvil poses a threat to the energy sector, in particular.

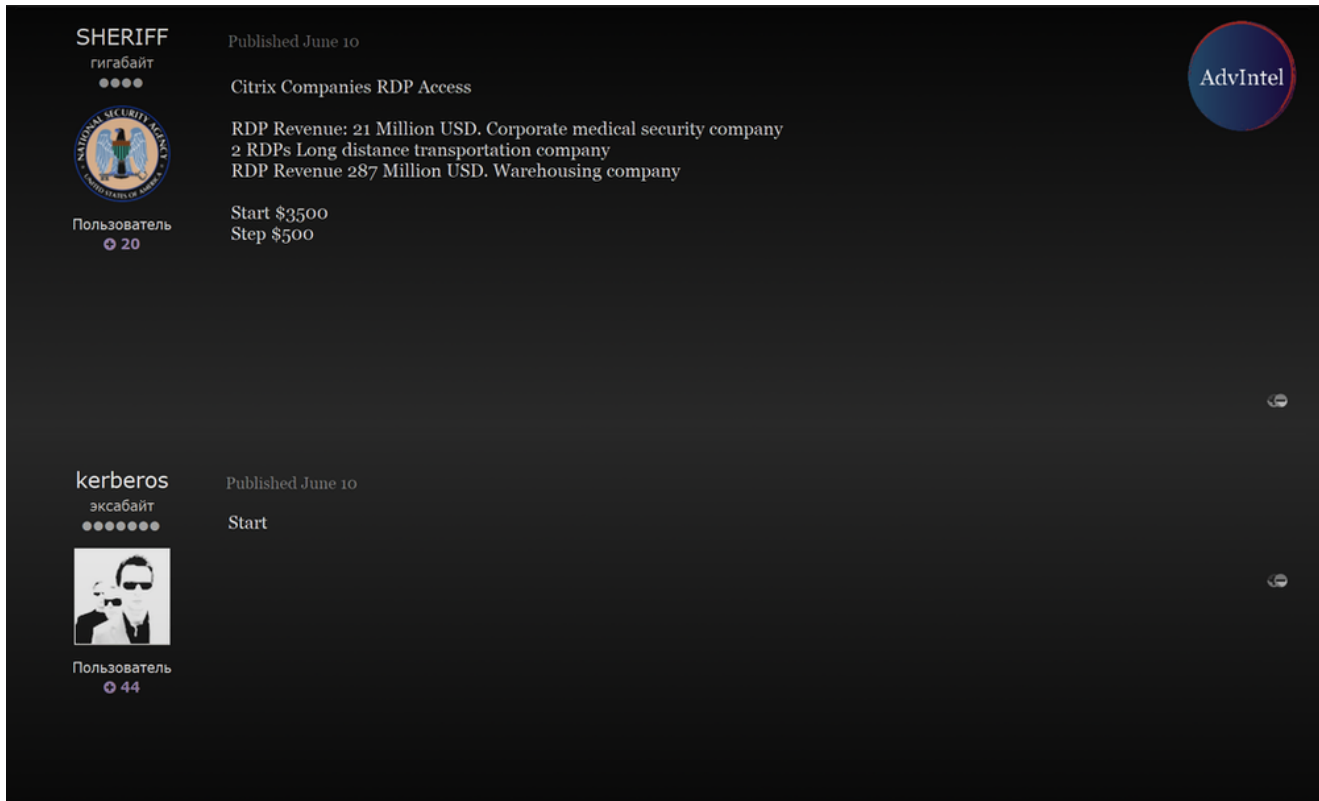


Image 4: A high-profile REvil affiliate purchases SHERIFF Citrix access.

The threat actors’ other solicitations have focused on the e-commerce, financial, and healthcare industries, and as a result, AdvIntel believes that REvil poses a credible threat to these industries, as well. It should be noted, however, that the threat REvil poses to victims goes beyond data encryption; REvil has been known to exfiltrate data to a public-facing blog, indicating that even prepared with data backups, companies can still risk reputational damage in the event of an attack.

Conclusion

REvil’s recent activities in the cybercriminal underground significantly alter the ransomware threat landscape.

Its interactions with high-profile threat actors suggest a preference to work as part of a network intrusion-focused criminal syndicate, which is an entirely novel business model to a Russian-speaking ransomware community historically reliant on mass spearphishing. The group's interactions with top-tier threat actors such as "Sheriff" and "Kerberos" indicate a proclivity for RDP exploits, particularly in the energy sector, but also in finance, security, and education. Given REvil's targets' prominence and large revenue streams, it appears that REvil is now aiming for high-profile, high-reward attacks in critical industries.

Here are some possible steps entities can take to prevent attacks and mitigate consequences from REvil related breaches:

1. entities whose data/networks have already been compromised must notify users of the breach;
2. companies must ensure reliable backups of all system files and communications;
3. administrator rights should only be granted to users who absolutely require it;
4. antivirus software – as well as its source databases – must be updated to the latest version, and used to verify programs before executing them;
5. access to unused system directories must be restricted; and
6. firewalls must be installed on user workstations to filter incoming connections.

REvil has gained substantial notoriety in the cybersecurity world, both for its connections to GandCrab malware and for its own nefarious activities in the criminal underground. After likely learning from GandCrab on how to organize extended criminal networks, REvil is now enabled by other threat actors such as "Sheriff", who sells its network access, and "Kerberos", who allows REvil the privilege of its endorsement (and possibly, its affiliation).

In this way, REvil and the actors it interacts with form a cohesive, underground economy, in which victims – and the data they own – are the main commodity.

UPDATE: Image 1 of this report has been updated to correct a technical error. Image 1 illustrates that REvil does not only communicate with SHERIFF but is willing to pay a top price in order to purchase underground auction bids offered by this threat actor.