STRATEGIC ADVISORY

ZEROFOX



Ransomware Landscape

Table of Contents

Executive Summary 3

Key Points 3

Intelligence Requirements 4

Six-Month Ransomware Activity: New and Continued Threats 5
- New Threats 5
- Notable Past and Current Ransomware Threats 8

Repeat Ransomware Offenders 10

REvil 10

Ransomware and National Security 12

Cybercriminal Underground Network Activity 14

Recommendations 17

Conclusion 18

© 2021 ZeroFox Inc. All rights reserved.

Executive Summary

In the past six months, the ZeroFox Threat Intelligence team has observed the changing ransomware landscape with new, current, and evolved threats. As new threats emerged, current threats persisted or evolved to include novel capabilities and techniques. Among new threats included the discovery of Colossus ransomware by ZeroFox Threat Intelligence and new ransomware families based on old ransomware with a history of success. One of the most active ransomware groups since 2019, REvil was responsible for large-scale attacks on organizations around the world including the Kaseya supply chain attack. The media attention from such attacks led to some popular cybercriminal networks prohibiting the discussion of ransomware or affiliate programs from posting advertisements, as these networks are often monitored by security researchers and law enforcement. Furthermore, the fight against ransomware escalated as world leaders enacted legislation responding to ransomware attacks and sanctions on cryptocurrency exchanges used to pay ransom demands.

Key Points

- In the past six months, ZeroFox observed new ransomware families emerge that included novel, rebranded, or new versions of discontinued ransomware variants.
- Known ransomware families, like Conti and REvil, continued operations and were responsible for prolific attacks on organizations around the world.
- The REvil group's activity included large-scale attacks on Kaseya and JBS SA that gained significant attention from the media and the United States (US) federal government. REvil also exhibited a period of no activity before the US government announced the suspension of REvil's operations.
- A selection of popular cybercriminal networks and forums introduced bans on ransomware-related discussion and affiliate group advertisements, due to the attention from the media as well as law enforcement monitoring such networks.
- In response to attacks like Colonial Pipeline, JBS, and Kaseya, the US government introduced legislation to improve national cybersecurity through Presidential Executive Order 14028 and sanctions on cryptocurrency exchanges for ransomware as well as ransomware negotiation and payments.

This report is based on some open source findings. Therefore, the report is open source intelligence and does not constitute definitive evidence. Information found in the open source cannot necessarily be verified.

© 2021 ZeroFox Inc. All rights reserved.

Intelligence Requirements



Malware



Deep Dark Web & Criminal Underground



Vulnerability



PII & Fraud



Geopolitical & Physical



Brand

For the most up to date list of ZeroFox Threat Research's Intelligence Requirements, please visit:

https://cloud.zerofox.com/alpha_team/advisories/14956

© 2021 ZeroFox Inc. All rights reserved.

Six-Month Ransomware Activity: New and Continued Threats

New Threats

Within the past six months, new ransomware variants emerged on the threat landscape that involved novel, rebranded, and new ransomware based on existing variants. Three examples of prevalent ransomware from each group during this six-month time frame included LockBit 2.0, Colossus, and BlackMatter ransomware. All three variants are Ransomware-as-a-Service tools that use evolved ransomware extortion schemes.

LockBit 2.0

The LockBit 2.0 ransomware is an updated version of the LockBit ransomware, which was launched shortly after the LockBit team took a brief hiatus following large-scale ransomware attacks on US-based companies and increased attention from law enforcement. Operators advertised the updated version on their website in June 2021, with attacks ramping up in July 2021. The LockBit team has been active since 2019 and first participated in double extortion schemes in 2020. Unlike the previous version of LockBit, LockBit 2.0 has a faster and more efficient encryption method than other ransomware variants during that time frame. Another contrast from the original LockBit is that, in some instances, LockBit 2.0 changed the target machine's desktop wallpaper to a LockBit 2.0 advertisement that essentially recruits corporate insiders to join LockBit to breach and encrypt networks.[1]

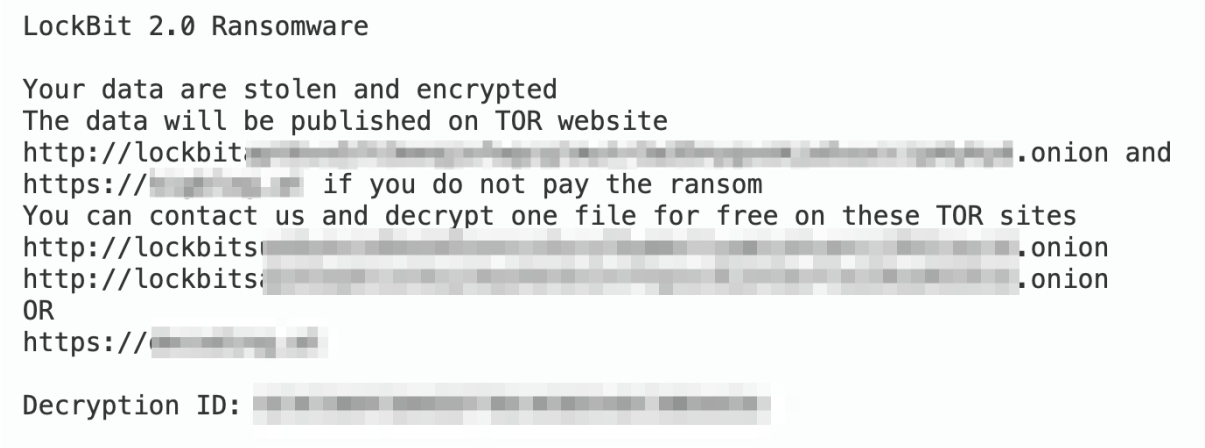


Figure 1. Example of LockBit 2.0 ransom note
Source: ZeroFox Threat Intelligence

Additionally, the operators opened a thread on a cybercriminal underground forum advertising an affiliate program for the LockBit 2.0 in June 2021 to cooperate with experienced penetration testers who have experience with Metasploit and Cobalt Strike. The operators also convey that

[1]hXXps://www[.]bleepingcomputer[.]com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

© 2021 ZeroFox Inc. All rights reserved.

LockBit 2.0 does not function in post-Soviet Union countries, which includes countries in the Commonwealth of Independent States.

Colossus

One of the many new ransomware variants within this six-month window was the Colossus ransomware. ZeroFox discovered Colossus ransomware after a Colossus binary was uploaded to an online malware sandbox platform on September 24, 2021. Because there was no information publicly available on Colossus, ZeroFox performed preliminary analysis on the binary and observed that it was protected with Themida, a well-known packer that can make use of virtualization techniques and anti-sandbox measures to make static binary analysis significantly more challenging. Furthermore, ZeroFox observed that the Colossus ransom note borrowed elements from existing ransomware families, like REvil, EpsilonRed, and BlackCocaine. This could indicate using a similar builder for the ransomware files and follows a pattern of ransomware groups disappearing and reappearing with a rebranded name and similar toolsets.

[+] What's Happened? [+]

Your files have been encrypted and currently unavailable. You can check it. All files in your system have "Colossus" extension. By the way, everything is possible to recover (restore) but you should follow our instructions. Otherwise you can NEVER return your data.

[+] What are our guarantees? [+]

It's just a business and we care only about getting benefits. If we don't meet our obligations, nobody will deal with us. It doesn't hold our interest. So you can check the ability to restore your files. For this purpose you should come to talk to us we can decrypt one of your files for free. That is our guarantee.
It doesn't metter for us whether you cooperate with us or not. But if you don't, you'll lose your time and data cause only we have the private key to decrypt your files. time is much more valuable than money.

[+] Data Leak [+]
We uploaded your data and if you dont contact with us then we will publish your data.

[+] What's Happened? [+]

Your files have been encrypted and currently unavailable. You can check it. All files in your system have {EXT} extension. By the way, everything is possible to recover (restore) but you should follow our instructions. Otherwise you can NEVER return your data.

[+] What are our guarantees? [+]

It's just a business and we care only about getting benefits. If we don't meet our obligations, nobody will deal with us. It doesn't hold our interest. So you can check the ability to restore your files. For this purpose you should visit our website where you can decrypt one file for free. That is our guarantee.
It doesn't metter for us whether you cooperate with us or not. But if you don't, you'll lose your time and data cause only we have the private key to decrypt your files. In practice - time is much more valuable than money.

[+] How to get access to our website? [+]

Figure 2. A side-by-side comparison of Colossus (left) and REvil (right) ransom notes
Source: ZeroFox Threat Intelligence

Like many other ransomware groups, Colossus participates in extortion schemes by operating and maintaining a data leak website. The ransom note discovered by ZeroFox included a reference to the targeted victim of the Colossus sample, a US-based automotive company. On October 14, 2021, ZeroFox observed the launch of a Colossus data leak website containing a single entry for the compromised automotive company.

© 2021 ZeroFox Inc. All rights reserved.



Figure 3. Colossus victim entry on data leak website
Source: ZeroFox Threat Intelligence

BlackMatter

BlackMatter is based on the DarkSide ransomware which was responsible for the Colonial Pipeline attack in May 2021. After the Colonial Pipeline attack made significant media headlines and caused gasoline shortages in parts of the US, DarkSide operators opted to keep a low profile due to the attention from the attack. Soon after, DarkSide reportedly lost access to their data leak website and servers causing the team to halt operations. During this window of minimal DarkSide activity, operators launched BlackMatter as the successor to DarkSide in July 2021. BlackMatter has been responsible for primarily targeting and publicly shaming US-based organizations – approximately 63% according to ZeroFox research.

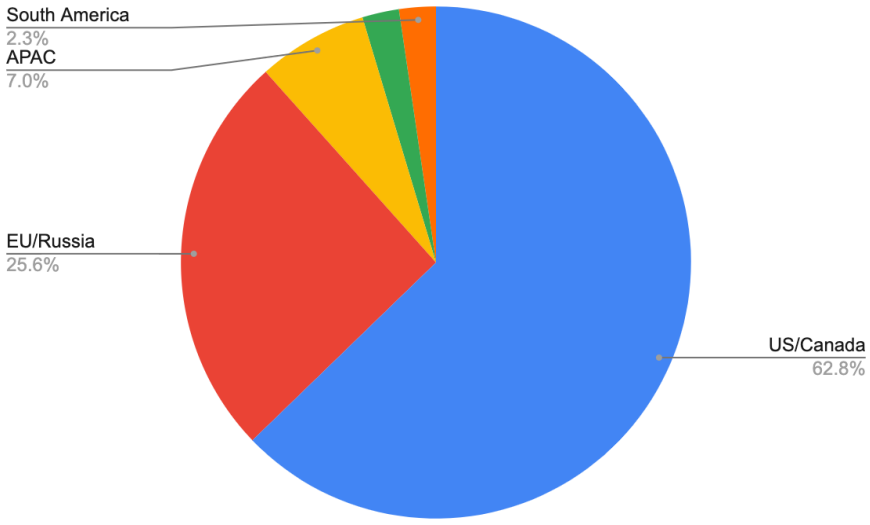


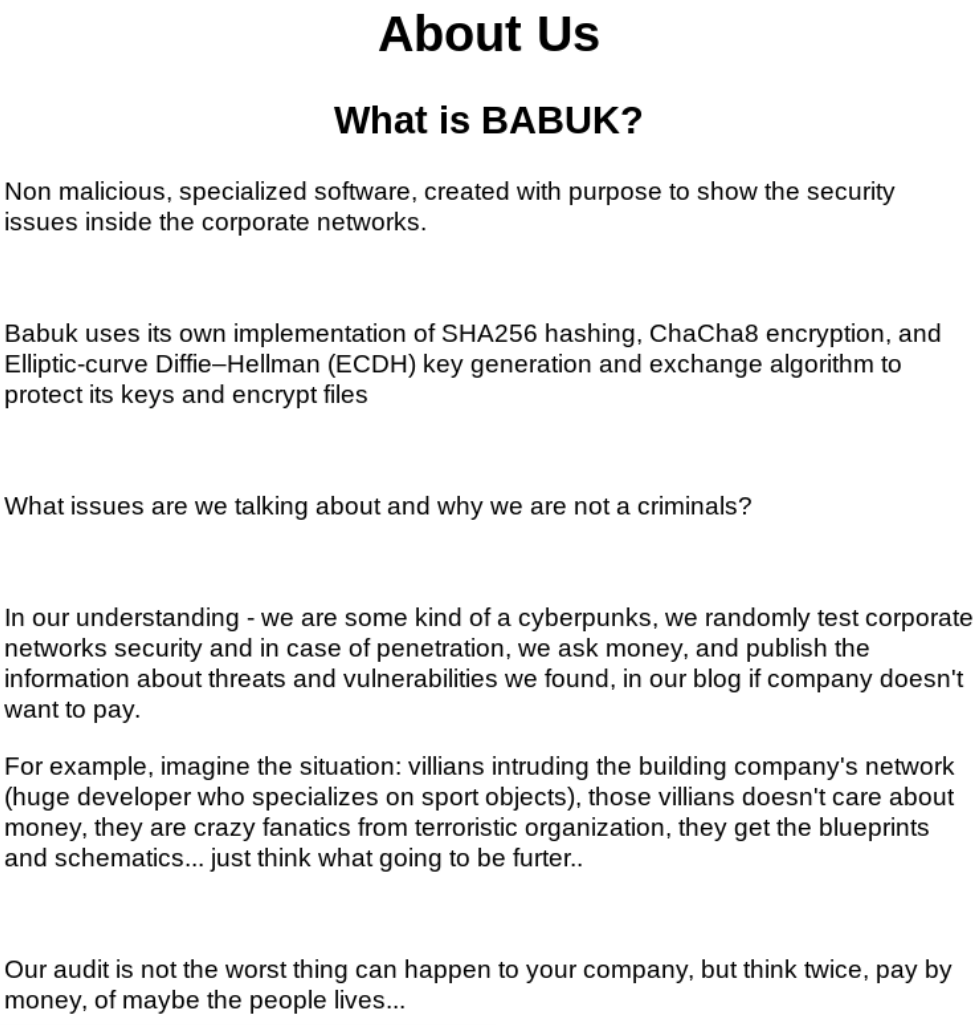
Figure 4. BlackMatter victims based on target region
Source: ZeroFox Threat Intelligence

© 2021 ZeroFox Inc. All rights reserved.

Notable Past and Current Ransomware Threats

Babuk

Babuk ransomware was first discovered in early January 2021. In its early days, victim leaks and updates from the actors were posted on underground criminal forums before launching a data leak website. After the first researchers began to publish their analyses of the ransomware, Babuk representative biba99 made a large post to Raid Forums to "express our great gratitude to all security researchers that they are studying our product..." The post then goes on to describe Babuk as "non malicious, specialized software, created with the purpose to show the security issues inside the corporate networks."



About Us

What is BABUK?

Non malicious, specialized software, created with purpose to show the security issues inside the corporate networks.

Babuk uses its own implementation of SHA256 hashing, ChaCha8 encryption, and Elliptic-curve Diffie–Hellman (ECDH) key generation and exchange algorithm to protect its keys and encrypt files

What issues are we talking about and why we are not a criminals?

In our understanding - we are some kind of a cyberpunks, we randomly test corporate networks security and in case of penetration, we ask money, and publish the information about threats and vulnerabilities we found, in our blog if company doesn't want to pay.

For example, imagine the situation: villians intruding the building company's network (huge developer who specializes on sport objects), those villians doesn't care about money, they are crazy fanatics from terroristic organization, they get the blueprints and schematics... just think what going to be furter..

Our audit is not the worst thing can happen to your company, but think twice, pay by money, of maybe the people lives...

Figure 5. Babuk "About Us" page on operators' data leak website
Source: ZeroFox Threat Intelligence

January 2021 through April 2021 saw several organizations fall victim to the group, including the Metropolitan Police Department of the District of Columbia. The attention from attacking the

© 2021 ZeroFox Inc. All rights reserved.

Metropolitan Police Department allegedly caused disagreements within the group over those who wanted to publish the leak and those who felt it went too far, eventually leading to a retirement announcement and the group's split. Payload.bin, a site focused solely on extortion, was launched as a direct result of the fallout.

Near the end of June 2021, a compiled version of the Babuk ransomware builder had been posted online for anyone to download. Finally, on September 2, 2021, a user going by the handle "dyadka0220" published the full source code for each version of the ransomware (ESXI, NAS, and Windows), their decryptors, and the builder application. Both leaks have resulted in new attacks using Babuk tooling with new branding. Incidents involving the leaked builder still had the ".babyk" file extension after encryption due to that not being a configurable option. ZeroFox also published an advisory for Delta Plus, a ransomware variant nearly identical to Babuk, save for its compilation timestamp and the encrypted file extension.[2]

Conti

Conti is another major ransomware-as-a-service (RaaS) group that has been active since mid-2020. An alert published by the Cyber Security & Infrastructure Agency (CISA) in September 2021 noted the group typically gains access to a network in several different ways.[3] Spearphishing campaigns, which are more targeted phishing attacks, are often used with malicious attachments or links to execute scripts or download other malware to assist in the attack. Stolen credentials are also often used to gain access through services like Remote Desktop Protocol (RDP) that have been exposed directly to the Internet. 2021 saw many vulnerabilities used by ransomware groups as well. Conti was observed using the PrintNightmare (CVE-2021-34527) and Zerologon (CVE-2020-1472) vulnerabilities.

Of all the RaaS groups observed by ZeroFox in 2021, Conti has the highest victim count thus far. Over 330 victims have been listed on the group's leak site in 2021, with 82 being published in the third quarter alone. At a time when most groups have set boundaries for industries that they will not attack, Conti continues to target victims in areas such as critical infrastructure, education, energy, and healthcare. One victim in the healthcare industry was attacked in May of this year. Conti eventually provided the victim with a decryptor for free, but held firm in demanding payment in return for not releasing any of the stolen data.

In August 2021, an alleged affiliate leaked what became known as the Conti "playbook." The leak contained several guides, videos, and tools for affiliates. The guides were meant to provide affiliates with everything they needed to get started, such as how to perform network reconnaissance, what information to look for on victim networks, how to escalate privileges, and steps for running the included tools. Most recently, in October 2021, Conti has begun threatening to immediately drop negotiations with victims and publish all of their data if a negotiation becomes public. The group immediately followed through on this threat by informing a then-negotiating victim that their data would be published.

[2] hXXps://cloud[.]zerofox[.]com/intelligence/advisories/15829
[3] hXXps://us-cert[.]cisa[.]gov/ncas/alerts/aa21-265a

© 2021 ZeroFox Inc. All rights reserved.

Repeat Ransomware Offenders

As ZeroFox Research observed in an advisory earlier this year, an interesting trend seems to be emerging in the ransomware world.[4] Some victims are being attacked multiple times. ZeroFox research has uncovered three victims at the time that were compromised two or more times in the span of the same month.

As we asserted at the time, there has been an increase in ransomware actors revisiting the same victims on multiple occasions, and since that time that percentage of attacks has increased. Our belief at the time that the Grief Ransomware group was a rebranding of the DoppelPaymer threat group has since been confirmed.

Rebranding and derivative actions also continue to contribute to the scale of the number of actors returning to the well of earlier success. With the emergence of actors like LockBit 2.0 rising from LockBit, BlackMatter showing ties to LockBit, REvil, and DarkSide, and Payload.bin and Babuk2.0 both deriving from the former Babuk team. But review of the activities of the new derivative and rebranded groups continue to follow the trend of attacking the same victims at a similar rate of the broad-view statistics for victims being attacked multiple times.

REvil

One of the most popular and persistent ransomware variants of over two years has been the REvil ransomware. REvil, also known as Sodinokbi, first emerged on the threat landscape in April 2019, as a successor to the GandGrab ransomware.[5] Towards the end of December 2019 and the beginning of January 2020, REvil gained significant attention for a large-scale attack on foreign-currency exchange company, Travelex, which was also the second ransomware group to utilize double extortion schemes in a ransomware attack.[6]

Fast forward to 2021, REvil continued to be a massive threat to organizations and individuals. In the past six months, known REvil infections on businesses peaked in June 2021 before dramatically decreasing when the group temporarily suspended operations in mid-July. In September, the team added new victim entries to their data leak site, although these entries were fewer in volume as this trend continued into October.

[4] hXXps://cloud[.]zerofox[.]com/intelligence/advisories/15323
[5]hXXps://www[.]darkreading[.]com/attacks-breaches/gandcrab-developers-behind-destructive-revil-ransomware
[6] hXXps://www[.]acronis[.]com/en-us/blog/posts/travelex-hit-powerful-sodinokibi-ransomware-attack/

© 2021 ZeroFox Inc. All rights reserved.

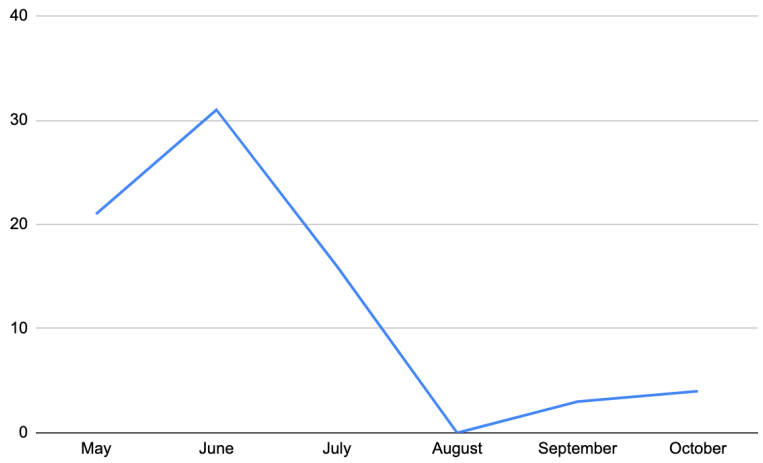


Figure 6. Volume of REvil targets based on data leak website
Source: ZeroFox Threat Intelligence

After increased attention on ransomware groups following Colonial Pipeline in May 2021, REvil maintained operations and avoided targeting US-based organizations as the US Department of Justice (DOJ) announced that they would elevate ransomware investigations to the same priority as terrorism. However, this changed after REvil targeted Brazil-based meat-processing company, JBS SA, in June 2021 that also affected JBS servers in the US and Australia.[7] Although a REvil spokesperson claimed that the intent was not to harm US-based operations, the US' response to form a stronger, strategic plan to fight ransomware attacks prompted the group to lift restrictions on US targets. In the following month, REvil conducted a massive supply chain ransomware attack on the Kaseya managed service provider.[8] Although the attack may have affected a small number of Kaseya clients, the majority of the attack affected small and midsize businesses that use the company's services as part of their operations. A universal decryption key was later released on cybercriminal underground networks for victims of the Kaseya attack, and security researchers confirmed that the key would not work on non-Kaseya REvil-encrypted machines.

After the Kaseya attack, REvil operators temporarily shut down operations in mid-July 2021. Security researchers believed that the group terminated for good or took a hiatus to update or rebrand REvil. Both cases proved false as the group resurged in September 2021 with minimal activity. On October 17, 2021, an alleged REvil associate posted a thread on a Russian-speaking forum claiming that a third party, "with the same keys" as REvil team members, had unauthorized access to the REvil data leak site and infrastructure. The party compromised the server and prevented access from REvil team members.

[7] hXXps://www[.]npr[.]org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says
[8] hXXps://www[.]zdnet[.]com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

© 2021 ZeroFox Inc. All rights reserved.

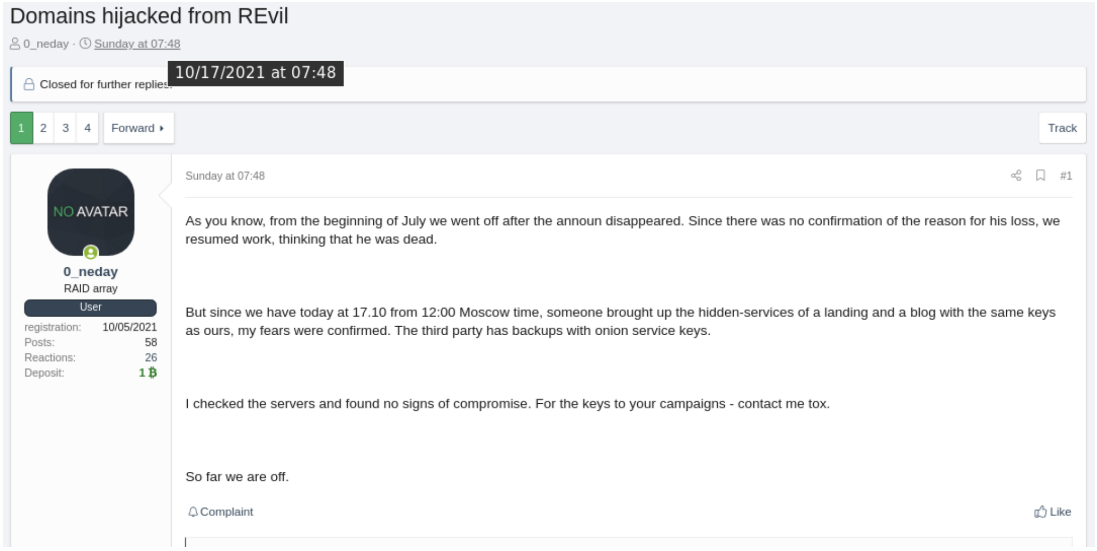


Figure 7. An alleged REvil member claims REvil servers have been compromised
Source: ZeroFox Threat Intelligence

On October 21, 2021, the US DOJ, in conjunction with other agencies, suspended REvil operations days after the October 17th forum post.[9] Although this is a significant win for cybersecurity organizations, law enforcement, and ransomware targets, a common trend among ransomware groups is to create new ransomware from old variants with a known history of success. This is especially true if the source code for an existing ransomware sample becomes public for threat actors, as well as security researchers for defensive measures. Additionally, some ransomware operation groups frequently advertise recruitment opportunities for affiliate groups, which may involve threat actors with experience working on ransomware and other malicious tools.

Ransomware and National Security

In the US, the Biden Administration enacted a number of policy initiatives designed to disrupt or otherwise affect ransomware operations against victims within the nation's borders. Those initiatives took a number of different forms and addressed the problem from several different vectors. One policy targeted the government infrastructure, one policy targeted the financial transactions, and one initiative focused on international cooperation.

On March 29, 2021, President Biden signed a one year extension to the national emergency condition described in Executive Order (EO) 13694 (originally enacted in 2015), including its updates referenced in Executive Order 13757 (enacted in 2016).[10] In addition to that action, the Biden Administration launched EO 14028 on May 12, 2021, with the goal of improving the

[9]hXXps://www[.]reuters[.]com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/
[10]hXXps://www[.]whitehouse[.]gov/briefing-room/presidential-actions/2021/03/29/notice-on-the-continuation-of-the-national-emergency-with-respect-to-significant-malicious-cyber-enabled-activities/

© 2021 ZeroFox Inc. All rights reserved.

nation's cyber security posture.[11] The directive outlines a number of different guidelines on improving sharing of cyber threat intelligence between the Intelligence Community and government agencies and departments.

EO 14028 describes a 120 day plan for implementing improved data sharing and preservation guidelines within the US Government, Intelligence Community, and private industry. It additionally outlines a 180 day plan towards the wide adoption of Zero-Trust Architecture, Multi-Factor Authentication, data encryption at-rest and in-transit, and implementation of cloud security designs using Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS). Furthermore, it lays out a 1 year timeline for the improvement of Supply Chain Security. In the order's other sections they go on to establish a Cyber Safety Review Board within the Department of Homeland Security, direct the creation of standardized playbooks for cybersecurity vulnerabilities and incidents, assign responsibilities for improving the federal government's vulnerability and incident response process, and describe requirements for system logging and retention.

Pursuant to the direction communicated by the White House, the Department of the Treasury issued a press release regarding their plans for actions against the growth of ransomware.[12] The first action involved the sanctioning of the SUEX virtual currency exchange, prohibiting US persons or entities from engaging in any transactions with them. The action was not against all cryptocurrency exchanges nor all RaaS providers, but it was an indication of how the department intends to conduct such dealings in the future. In that same press release, the department announced an update to the policy regarding potential sanctions risks from paying ransoms.[13] The position is that the payment of ransoms is still highly discouraged, and reinforces that payment of ransoms could be viewed as providing material support to criminals. The letter ends on a declaration of the level of international cooperation involved in countering the ransomware threat.

On October 13, 2021, reinforcing the idea of international opposition to the threat of ransomware, President Biden hosted a 30-nation virtual summit. While the full analysis of the outcomes of the meetings is still ongoing at the time of this writing, there was significant agreement that ransomware is a transnational threat, that it is a threat that rises above the level of simple criminal activity and into the level of national security and infrastructure threats, and that there should be a significant increase in multinational disruption efforts and cooperation the like of which have occurred several times through the last year. It seems important to note that neither China nor Russia were invited to participate, despite their size and global influence. The White House is, however, in high-level discussions with both nations on the topic of cyber security.

[11] hXXps://www[.]whitehouse[.]gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[12] hXXps://home[.]treasury[.]gov/news/press-releases/jy0364
[13] hXXps://home[.]treasury[.]gov/system/files/126/ofac_ransomware_advisory[.]pdf

© 2021 ZeroFox Inc. All rights reserved.

Cybercriminal Underground Network Activity

Throughout 2020 and 2021, ransomware continually matured into a severe threat to organisations through the use of sophisticated attack chains and double extortion tactics. Many ransomware groups emerged during this time, with many operating data leak sites to pressure their victims, threatening to release their data if ransom demands were not met within a given timeframe, or if the victim enlisted outside assistance with negotiations. With ransomware groups continuing to see considerable ransom payouts, many groups increased their presence in criminal dark web forums and networks, looking for new opportunities and potential victims.

In the wake of the Colonial Pipeline ransomware attack, the RaaS ecosystem saw many changes.[14] As the initial disruption of the attack was controlled, US government agencies squarely set their sights on ransomware groups and their affiliates, prompting many to drastically change their operations and presence on the cybercriminal underground networks and communities. Subsequently, the RaaS group responsible for the attack, DarkSide, went so far as to entirely rebrand their operations under the new name BlackMatter. It is not uncommon for RaaS groups to close and reopen under a new name when they are receiving increased attention.

Many RaaS groups operate using an affiliate model, where third parties can use the group's software and infrastructure to facilitate ransomware attacks. This is done in exchange for a percentage of any ransom payout from the victim. Affiliates would often be accepted with little to no restrictions in regards to what sector the affiliate could target. However, the attack on Colonial Pipeline highlighted the risks, for both RaaS operators and governments, with targeting critical infrastructure.

In response to the actions and proposals from the US government, many criminal dark web forums which facilitated RaaS advertising and business operations, promptly banned any and all posts regarding ransomware operations. It is likely forum owners and administrators were concerned about the potential repercussions of facilitating these types of operations, as well as attempting to reduce further attention being brought to these cybercriminal networks.

[14] hXXps://cloud[.]zerofox[.]com/intelligence/advisories/14969

© 2021 ZeroFox Inc. All rights reserved.

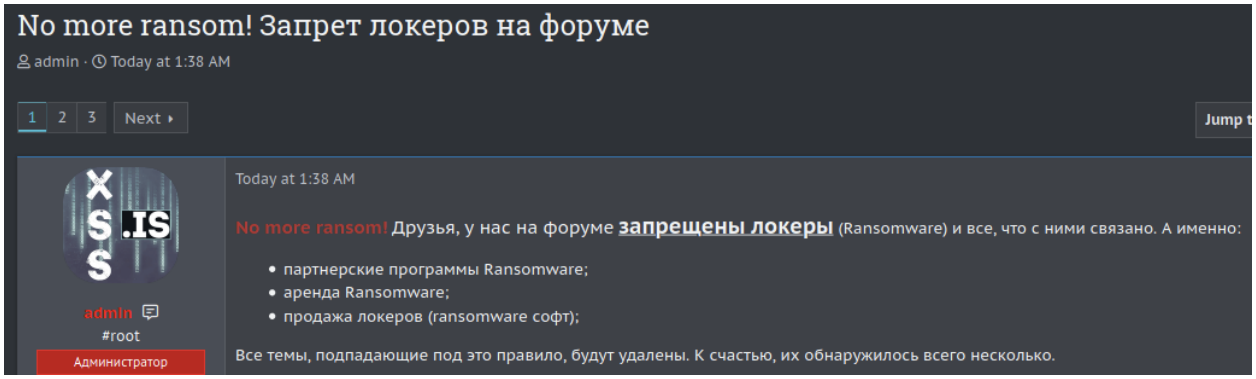


Figure 8: Snippet of forum administrator announcing a ransomware-related ban on a popular Russian-speaking forum
Source: ZeroFox Threat Intelligence

English translation of Russian text:

No more ransom! Banning lockers on the forum
Thread starter admin Start date Today at 1:38 AM
#one

No more ransom! Friends, on our forum lockers (Ransomware) and everything connected with them are prohibited. Namely:

Ransomware affiliate programs;
Ransomware rental;
sale of lockers (ransomware software);

All topics matching this rule will be removed. Fortunately, only a few of them were found.

Established RaaS groups such as BlackMatter and REvil introduced additional restrictions for affiliates, stating that attacks targeting specific sectors were now prohibited. Typically, these restricted sectors included government, healthcare, and educational institutions, or any business which falls under their countries definition of "critical infrastructure." This evidenced the changing climate for RaaS groups, and their willingness to alter business practices in order to retain their presence in key dark web criminal networks.

Conversely to this, other groups such as Conti did not alter their activities, and continued to target industries without restriction. This resulted in such groups having a much higher infection rate and target count than their counterparts which adopted more due diligence around their targets.

Due to many of the more popular RaaS groups closing their doors to new affiliates, or introducing more stringent controls around who they would work with, there was also a noticeable upward trend of new individuals and ransomware authors selling RaaS offerings in

© 2021 ZeroFox Inc. All rights reserved.

order to fulfil the growing demand in the market. Many of the new services being offered were smaller in scale, and instead of opting for an affiliate model, simply selling individual builds of their ransomware for a one-time payment.

In July 2021, ZeroFox observed the former Babuk and Payload.bin leak site change to a ransomware-focused forum named "RAMP." The administrator of this new forum, named "Orange," directly called out that the forum was specifically created due to other dark web networks banning ransomware related posts and threads. Since its creation, RAMP has seen a rapid adoption from new and established RaaS groups, network access brokers, and affiliates.

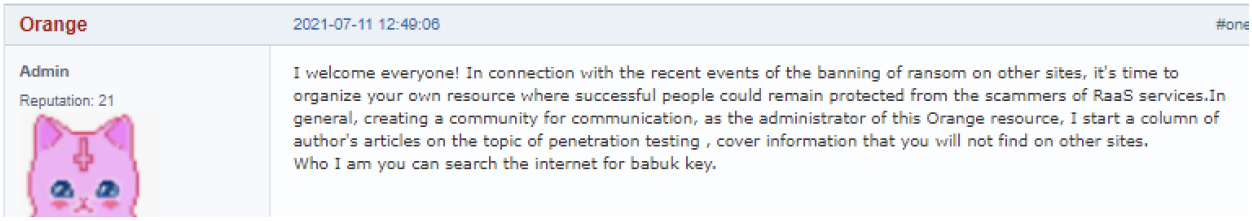


Figure 9. Forum administrator, "Orange," published a post on new RAMP forum, shortly after ransomware ban on popular forums
Source: ZeroFox Threat Intelligence

© 2021 ZeroFox Inc. All rights reserved.

Recommendations

- Ensure antivirus and intrusion detection software is up-to-date with all patches and rule sets.
- Enable 2-factor authentication for all of your organizational accounts.
- Utilize account permissions best practices such as role-based access control, least privilege, and restricting root/admin permissions.
- Segment critical network resources using zero-trust configurations.
- Maintain regularly scheduled backup routines, including off-site storage and integrity checks.
- Limit file egress by size and type.
- Avoid opening unsolicited attachments and never click suspicious links
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity.
- Consider disabling, or at least logging, all network activity outside of normal business hours for most users where possible.
- If a workstation is infected with malware, quarantine it on a private network segment with no external connections.
- If you are alerted or suspect a compromised account, change the password immediately.
- Disable unneeded protocols on your network (UDP, IPX, NetBIOS) and monitor for any use of them.
- Monitor usage of dual purpose tools such as Powershell for abnormal behaviors.
- If not already enabled, turn on the compromised credentials rule for all relevant entities and ensure relevant emails are entered for those entities, or reach out to ask@zerofox.com for assistance.
- Reach out to your ZeroFox account manager or ask@zerofox.com if you need help setting up monitoring, configuration or want more information about the associated website.

© 2021 ZeroFox Inc. All rights reserved.

Conclusion

Ransomware once more proves to be a persistent threat to businesses and individuals. In the last six months, the ransomware landscape exhibited significant activity that demonstrates how threat actors quickly adapt to an evolving market. The emergence of new, updated, and rebranded families highlights how ransomware operators shift from one RaaS to another due to improved capabilities and lucrative opportunities. Meanwhile, as threats like Babuk discontinued operations, the Conti group continues to thrive and target any organization that falls victim to their attacks. Cybercriminal underground marketplaces and networks offer a glimpse into some ransomware groups' operations, involving recruitment opportunities for affiliate programs and advertisements for malicious tools and services. Additionally, the actions, sanctions, and policies from federal governments to mitigate ransomware threats prompted some ransomware groups to keep a low profile and cybercriminal forum administrators to propose bans on ransomware-related discussions. Nevertheless, operators found new ways to resume nefarious activities despite increased attention from governments, law enforcement, and security experts. One fact is certain: ransomware operations will not halt any time soon, and as a result, organizations must remain vigilant of the evolving landscape.

Information Cut-Off Date: October 31, 2021

© 2021 ZeroFox Inc. All rights reserved.