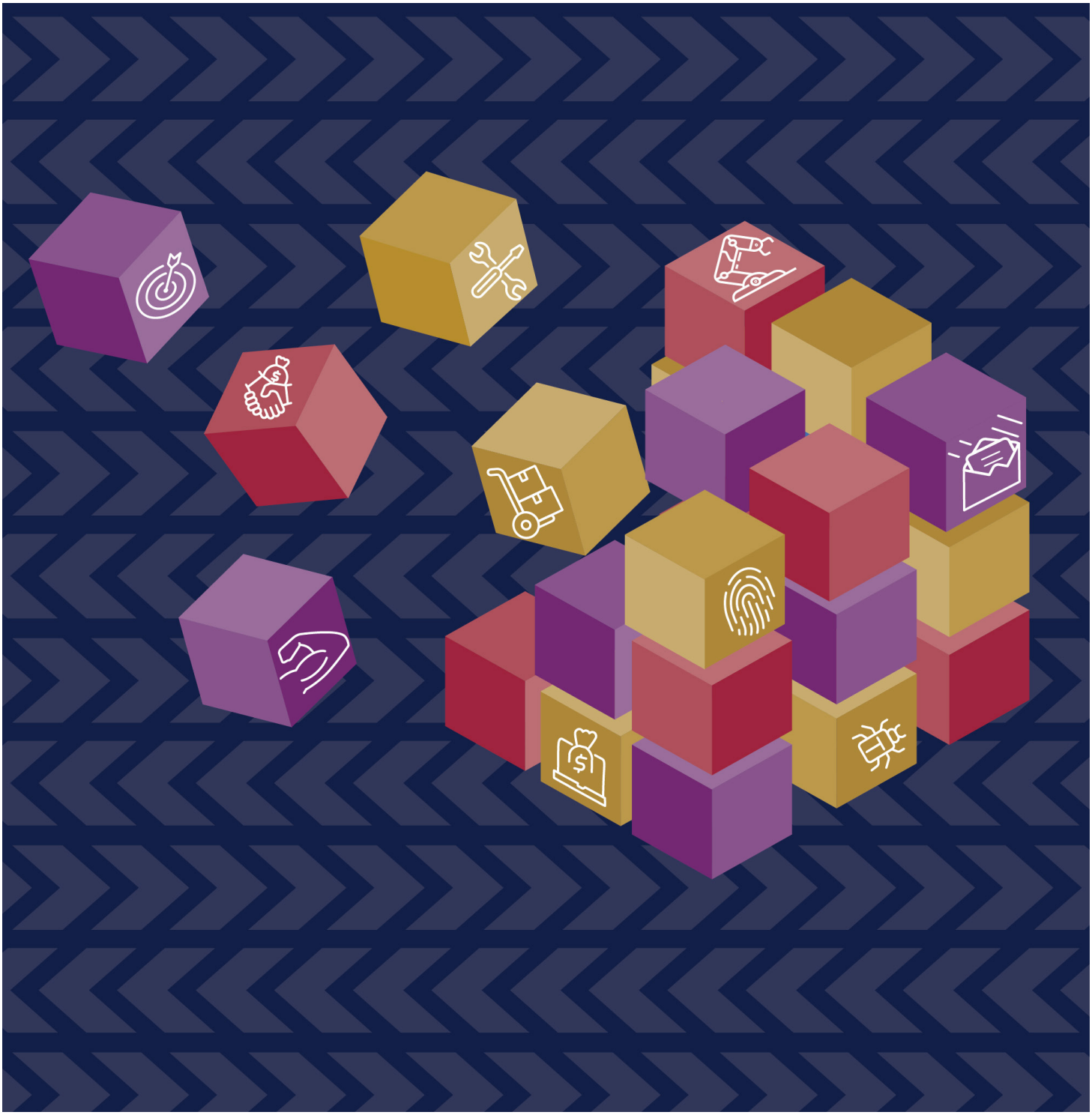
National Cyber Security Centre
a part of GCHQ

NCA
National Crime Agency

Ransomware, extortion and the cyber crime ecosystem

A white paper from the NCSC and the NCA.



MINISTERIAL FOREWORD

The UK is a high value target for cyber criminals.

Our businesses and institutions are among the foremost in the world, meaning they have three things that hostile cyber actors crave – money, information and the potential to cause widespread disruption if things go wrong.

Attacks against our citizens are also evolving, both in terms of scale and harm. In the last year there were an estimated 745,000 computer misuse offences. Criminality like this helps facilitate economic crime, such as fraud, and interpersonal crimes, such as stalking and domestic abuse.

Thankfully, our cyber and law enforcement agencies are also amongst the best in the world. This report was written to give you an invaluable overview of the threats we all face.

You will see that the threat picture has changed substantially since the publication of a previous report in 2017. It is easier than ever for those with malicious intent to cause huge disruption. The rollout of ransomware as a service means an advanced knowledge of computing is no longer needed to reap havoc; criminals are able to access software that will do much of the hard work for them.

This all means that it has never been more important to adopt good cyber hygiene. To get the most out of this paper, you should read it alongside the NCSC's Cyber Essentials programme[1], a scheme which provides expert advice and accredited training to protect businesses and institutions from a cyber attack.

The onus, of course, is not just on you. I am ensuring our agencies collaborate with our international partners to target cyber criminals, put a stop to their practices and hold them accountable.

And they are making progress.

This year we enforced two comprehensive sanction packages against more than a dozen Russian-speaking cyber criminals who targeted institutions across the world, including the NHS during the height of the pandemic.

The National Crime Agency worked alongside the FBI and German law enforcement to shut down a ransomware service, known as HIVE, which over two years extorted more than $100 million in ransom payments.

And we worked with 17 countries to take the Genesis Market (a go-to service which sold the personal data of millions of people to fraudsters) offline.

I will continue to do everything in my power to protect our cyber infrastructure – but you too must play a role. I hope you find this report useful as you seek to better understand and protect yourself against the threat we face.

The Rt Hon Tom Tugendhat, Minister of State (Minister for Security)

NCSC CEO FOREWORD

When it comes to cyber security, a lot can change in six years.

In 2017, the National Cyber Security Centre (NCSC) published a detailed report examining the cyber crime business model. Since then, the growth in ransomware and extortion attacks has expanded dramatically, with cyber criminals adapting their business models to gain efficiencies and maximise profits.

This white paper, published by the NCSC in conjunction with the National Crime Agency (NCA), examines how the tactics of organised criminal groups have evolved as ransomware and extortion attacks have grown in popularity.

Since IT systems are now ubiquitous, ransomware attacks can be truly devastating for victims and their customers, which is why it remains the most acute cyber threat for most UK businesses and organisations. Attacks can affect every aspect of an organisation's operation, hitting finances, compromising customer data, disrupting operational delivery, eroding trust and damaging reputations. The impact will be felt in the short and long term, particularly when organisations are unprepared. Recovery is often lengthy and costly.

As we shall learn, there are a number of enabling services, platforms, distributors and affiliates that are key to conducting a ransomware attack, and it's this wider cyber crime 'ecosystem' that is the focus of the paper, rather than the mechanics of ransomware itself.

The good news is that the NCSC and the NCA are helping organisations of all sizes to take responsibility for their own cyber security and improve their resilience. The paper explains that implementing NCSC ransomware guidance will interrupt the majority of attacks, which is why we encourage system owners and technical staff to explore the NCSC's ransomware pages[2].

The deployment of ransomware attacks relies on a complex supply chain, so focussing on specific ransomware strains can be confusing at best, and unhelpful at worst. We hope that the publication of this white paper shines a light on the motivations of the threat actors further upstream, who are ultimately driving the monetisation of ransomware as a service, and other extortion attacks.

Lindy Cameron, NCSC CEO

NCA FOREWORD

Ransomware continues to be the most significant, serious and organised cyber crime threat faced by the UK.

The reach and scalability of ransomware techniques, combined with dynamic adaptation by criminals, means that these crimes continue to have a significant impact in the UK and elsewhere. Consequences include a significant impact upon victims, disruption of services to the public, and compromise of personal data (which can be exploited for further criminality such as fraud).

The ransomware threat tends to manifest most obviously around data and system functionality, but we should also pay attention to societal harms, such as the overall confidence in the integrity, reliability and safety of our networked economy.

The ransomware threat has not stood still. To survive in a climate of heightened pressure from governments and law enforcement agencies, it has had to evolve and adapt. While individual groups have had to cease operation, as a whole the criminal industry is effective at amending its activities and business models dynamically to efficiently extract funds from victims.

Specialisation within the ecosystem, particularly 'Ransomware as a Service' and the proliferation of easily-used tools, online marketplaces and forums, has lowered barriers to entry.

The NCA's National Strategic Assessment 2023[3], notes that "Russian-language criminals operating ransomware as a service continue to be responsible for most high profile cyber crime attacks against the UK. Some of these high profile Russian-language groups are known to have links with the Russian state. However, it is highly likely that in most instances these links extend only to tolerance of their activities."

'Whole of system' response

Ransomware is fundamentally about criminal monetisation of cyber vulnerabilities. The most effective systemic response is preventing future attacks by investing in increased resilience and better protected systems. Companies and public sector bodies can justify these investments partly by observing the cost of ineffective cyber security. Complementing this key aspect of preventative work, the NCA also runs Cyber Choices campaigns[4] to help people in the UK avoid being drawn into cyber crime.

The factors set out above mean an investigative response to an individual ransomware attack will rarely be productive in itself. Instead our disruption strategy, complementing efforts to build resilience, is based on understanding and undermining the increasingly sophisticated criminal ecosystem behind these threats especially focusing on common enablers and vulnerabilities. This is an integral part of the NCA's broader shift of 'focus upstream, overseas and online', degrading the most harmful organised criminal groups (OGCs) by targeting those at the top of the chain, tackling the threat at source, and combating their use of technology.

Traditional criminal justice outcomes are hard to achieve against actors based in uncooperative jurisdictions. This puts a premium on a wider range of disruptive approaches including international cooperation to pursue criminals as and when opportunity arises. Advances in cryptocurrency analysis and other techniques have enabled actions against a range of historic cybercrimes. And the UK announced its first cyber sanctions, in conjunction with US partners, against 7 Russian ransomware criminals associated with the Conti-Trickbot group in February 2023[5].

The online cyber criminal ecosystem set out in this paper enables the scale of threat and harms within the UK itself. The NCA's National Cyber Crime Unit (NCCU) works with a wide range of partners in the UK and overseas to disrupt the key services that enable the cyber crime ecosystem; proactive, intelligence-led operational efforts, stressing the business model at multiple points with the overarching objective of achieving long-term strategic advantage.

The ransomware threat is borderless. An international response is needed to constrict the ecosystem that facilitates it. Our collective work with international partners includes private and public sector initiatives to make the UK's online environment more safe and secure, and ultimately a harder target for ransomware actors.

James Babbage, NCA Director General Threats

Contents

This white paper assumes an understanding of cyber security principles. It's particularly aimed at security professionals who need to be aware of changes in cyber criminal activity to better protect their systems and inform security policy.

Introduction

Ransomware has been the biggest development in cyber crime since we published the NCSC's 2017 report on online criminal activity.

Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A cyber criminal will then demand a ransom in exchange for decryption. The computer itself may become locked, or the data on it might be encrypted, stolen or deleted. The attackers may also threaten to leak the data they steal.

May 2021 saw a ransomware attack on the Health Service Executive of Ireland[6], causing issues such as lack of access to appointment data, in some cases leading to surgeons attempting to find patients for surgery when they had already been operated on. In the same month, the Colonial Pipeline in Texas[7] was also held to ransom causing major disruption to gas supplies across the east coast of the US. In the UK, ransomware attacks affected the critical care services provided by local councils, and multiple organisations in the education sector[8] were also affected.

As the ransomware threat has evolved[9], victims now have the worry of their sensitive data being exposed to the world, and with it face the risks of reputational damage. There will also be additional considerations of the impact of enforcement by a data protection authority (such as the Information Commissioner's Office in the UK) for not sufficiently protecting customer data.

More recently, some groups conduct data theft and extortion only, without deploying ransomware. Accordingly, cyber criminals will now use whichever approach they believe most likely to yield payment, deploying **ransomware attacks** to disrupt logistics companies that need the data to function, but favouring **extortion-only attacks** against healthcare services (where patient privacy is paramount).

Some criminal groups purport to follow a 'moral code' and avoid attacks against critical national infrastructure (CNI) and healthcare services. However, the reality of complex modern supply chains means criminals cannot know if their attack will impact such services.

The evolution of ransomware

While ransomware existed prior to 2017, it primarily focussed on encrypting single devices. In 2013, the GameOverZeus OCG had already put together the necessary success criteria for ransomware with CryptoLocker. It fused strong public key encryption with cryptocurrency payments, making it a viable business when other monetisation methods failed.

Damaging a large organisation's network (instead of a small organisation's or single user's) has become known as 'big game hunting'. These targets often involve higher payment demands and so a larger return on investment. The removal of access to critical business systems and/or data is used to demand payment in exchange for the recovery keys. Under these pressures, it's tempting for organisations to think that paying the ransom will 'make the incident go away', but as Eleanor Fairford, Deputy Director of Incident Management at the NCSC explained in a recent blog post, paying the ransom quickly doesn't always help[10].

Since 2018, businesses have been getting better at preparing for and responding to these attacks. At the same time, criminals have been refining their business model to maximise payouts. Combining data theft with extortion in big game hunting attacks increases the pressure on victims to pay, who will often be presented with short deadlines (a tactic often used in legitimate sales campaigns).

The WannaCry and NotPetya attacks combined encryption with the ability to self-propagate, leading to damages across a wide range of organisations. These attacks were both disruptive attacks posing as ransomware, in neither case was it possible to pay in exchange for decryption keys. However they highlighted the dramatic increase in impact when targeting critical infrastructure and large businesses. In 2018, the NCSC and the NCA observed this shift in criminal behaviour to conduct attacks against larger organisations, driven in part by the huge growth in the availability and legitimate trade of cryptocurrency.

Cryptocurrency has made it easier, cheaper and faster to obtain payment and purchase criminal services than was previously possible with traditional currencies. The use of cryptocurrency also makes it harder to attribute individuals and control illicit payments, although this is in the process of changing to match traditional currencies.

The cyber crime ecosystem

Most of the serious cyber attacks have traditionally been carried out by OCGs such as EvilCorp, which comprise highly organised criminals operating much like legitimate businesses with offices, salaries, holiday and sick pay, and other benefits. There's also a number of smaller, less-organised criminal groups and criminal microservices traded on illicit forums and marketplaces, all supporting each other.

While cyber crime exists in most countries around the world, the major threat to the UK emanates from the Russian-speaking community that have benefited from the larger OCGs helping shape the forums where these services are traded. Like other criminal services, ransomware has been adapting to this marketplace to become more accessible and scalable through groups selling ransomware as a service (RaaS). The resulting increase in criminals adopting ransomware and extortion tactics means that smaller criminal groups, working together, can make a large impact.

Sanctions, indictments and rewards levied on the likes of EvilCorp[11] (and the group behind Conti[11]) has seen them draw on the wider ecosystem to distance themselves from the larger OCG branding. Figure 1 is an estimate of the number of UK victims from the top 10 ransomware variants over the last 3 years. It shows that over time, some of the previously dominant groups (such as Conti and Egregor) have disappeared while more brands of 'as a service' data leak sites (such as ALPHV, Lockbit and Hive) have become available. The numbers here can only be taken as an indication of the true volume, as any victims that paid the ransom will not appear on the leak sites (and some ransomware variants do not adopt data leak tactics).

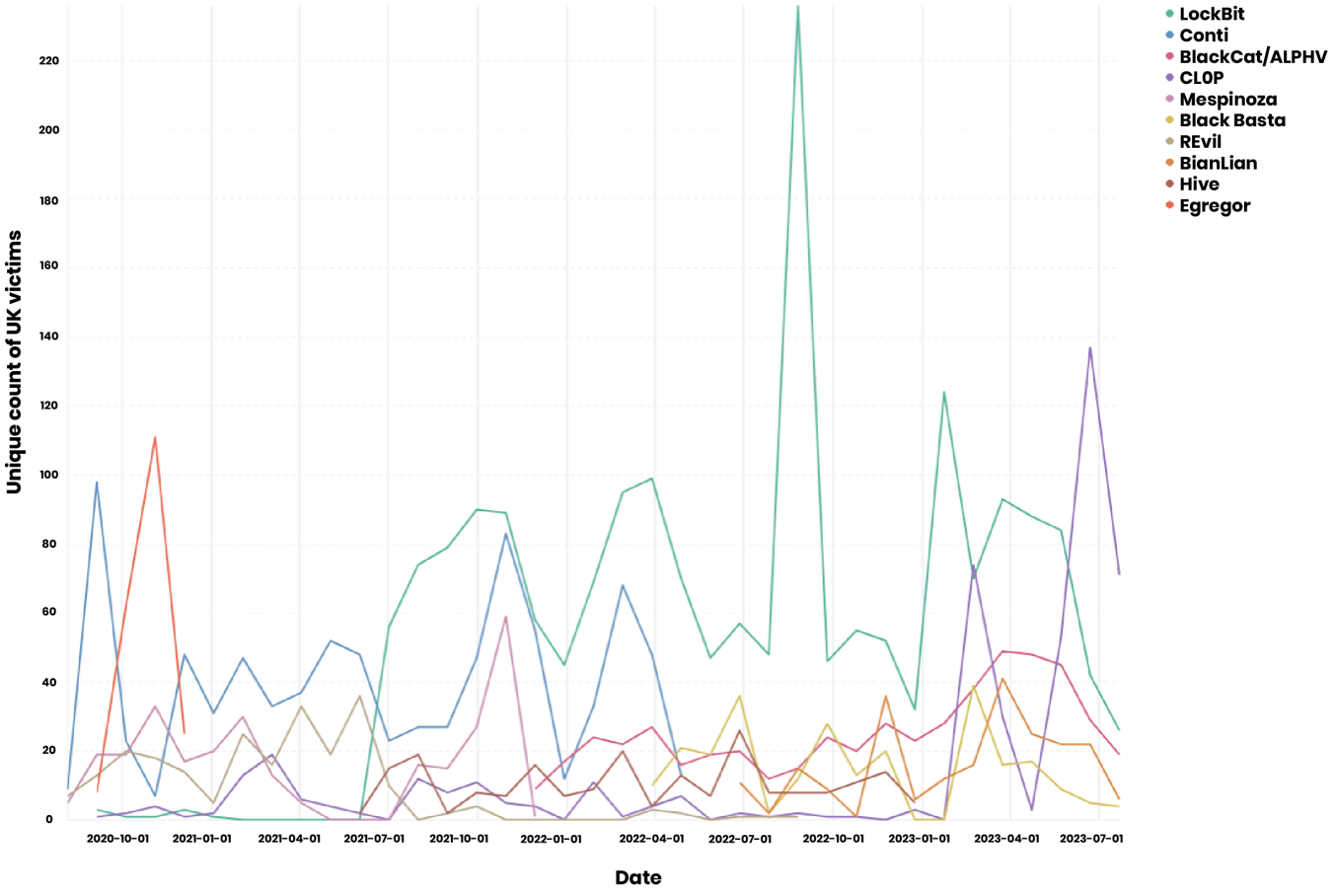


Figure 1. Data leak victims by leak site brand. Source: Secureworks

Despite the variety of criminal services available, there is a high level attack path for ransomware that can be broken into functions delivered by different malicious actors (Figure 2). The chronological flow of an attack is typically left to right, starting with an initial interaction with the victim on the left, and increasing in impact moving towards the right. In many cases, organisations are not aware that they have become a victim until the very end of this process.

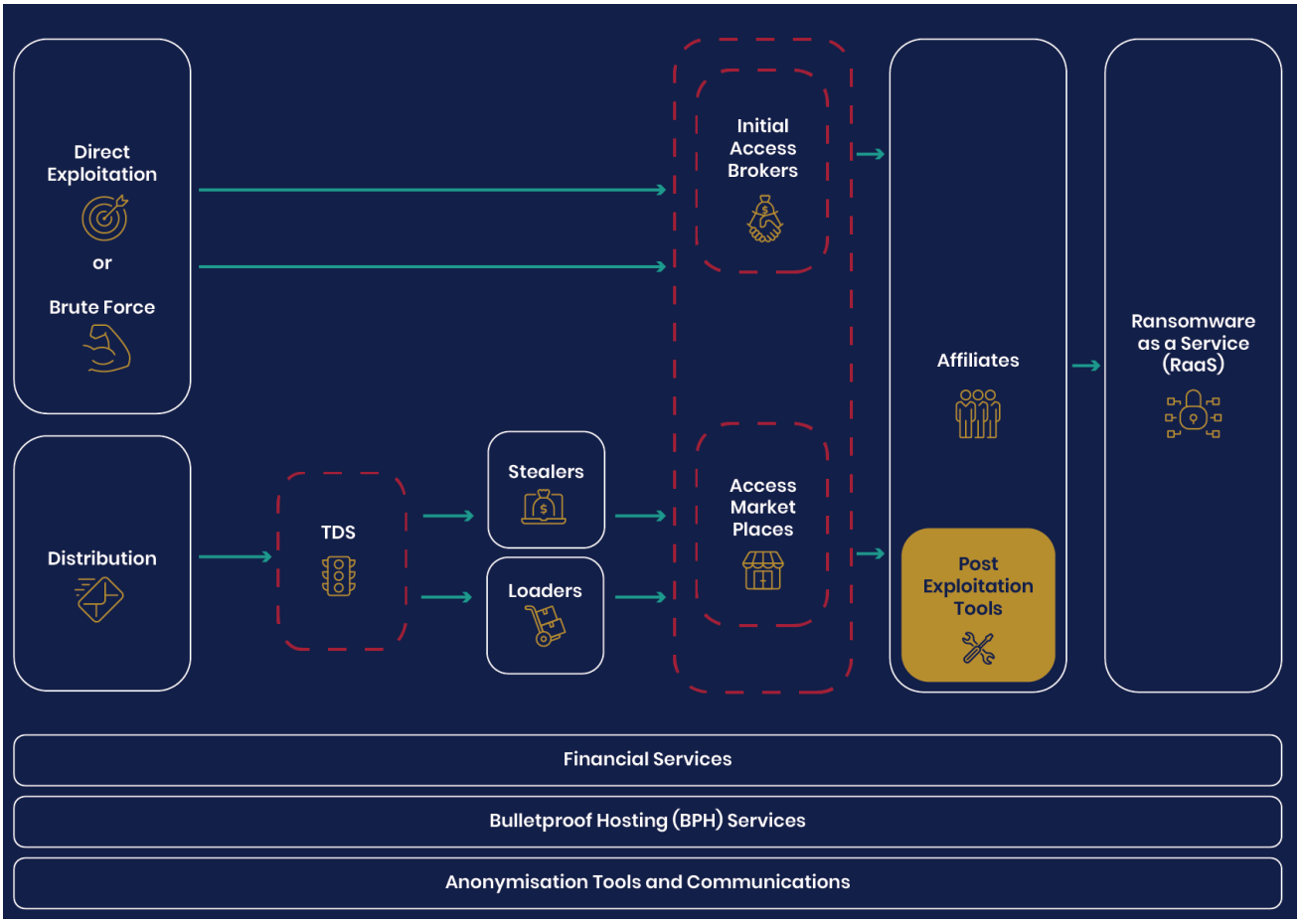


Figure 2. Simplified ransomware workflow

It's worth noting that:

- each function can be conducted by a different threat actor and sold to each other as a service
- malicious actors can execute more than one function themselves as fits their working methods, skills and capabilities
- some of these functions are also optional, such as TDS (Traffic Distribution Systems), which is used in some malware delivery, but not others.

This attack path is supported by a wide range of services, including criminal forums for discussing and exchanging services, anonymisation tools and malicious 'bulletproof' hosting that claim to provide infrastructure services that are resilient to takedown from law enforcement. Each of these underpinning services are necessary for the ecosystem to function but are outside the scope of this document.

Common initial access vectors

The left hand side of the diagram primarily deals with gathering initial accesses to targets, the trade of which constitutes much of the cyber crime ecosystem. Gathering these accesses can be done by dedicated access brokers, through online marketplaces, or by affiliates themselves. This flexibility makes it challenging for threat intelligence companies and defenders to understand which parts of the attack were conducted by which actor group. Attribution of a ransomware (or other cyber crime) incident to a single responsible actor is often impossible because of this business model.

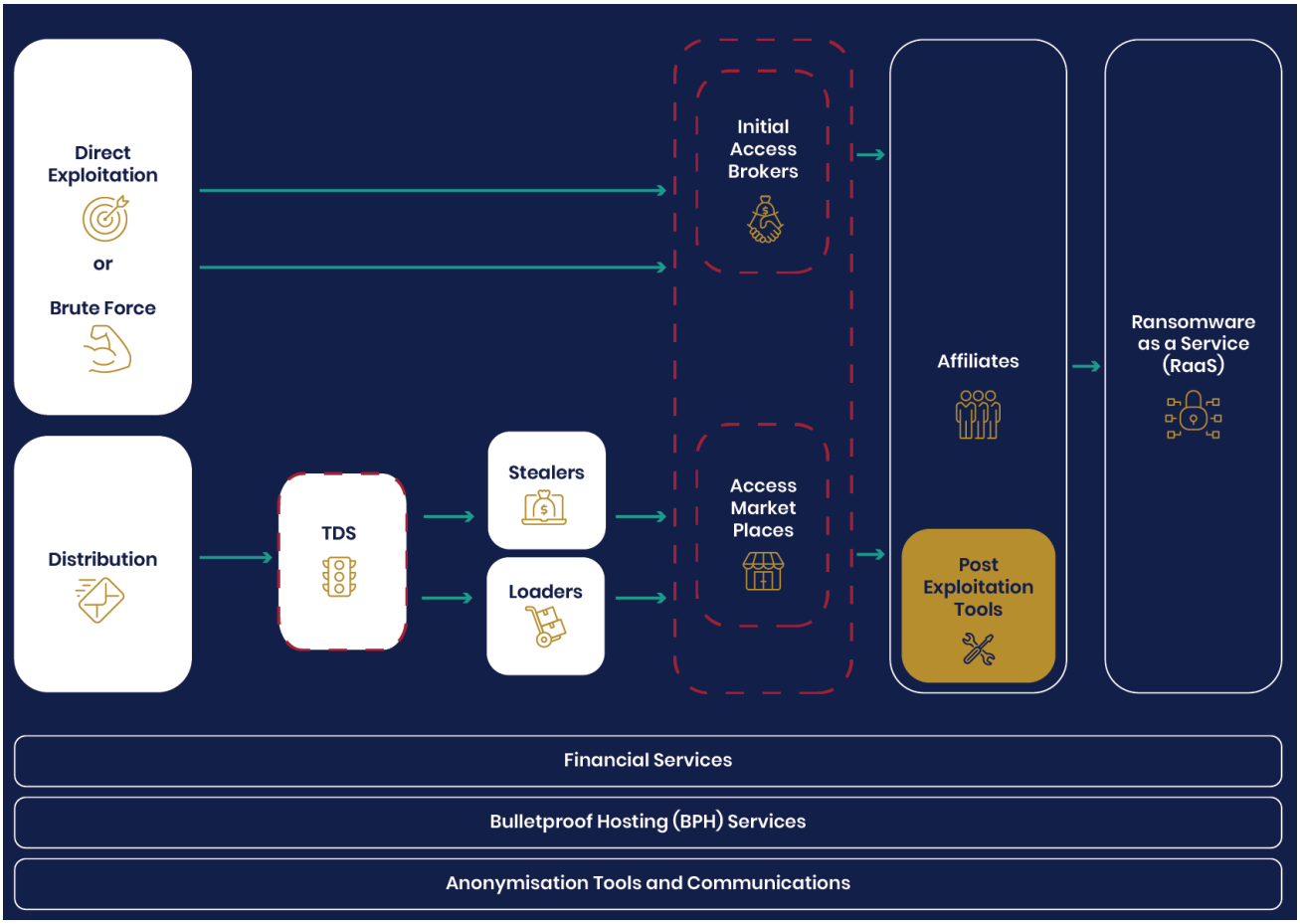


Figure 3. Common initial access vectors

It's important to note that **the majority of the initial accesses to victims are gained opportunistically and are not targeted against a particular organisation or business sector**. Cyber criminals are primarily concerned with financial benefit and while occasionally a group will specifically target sectors they have had previous success with (such as Vice Society and the education sector), the majority do not.

Headlines such as 'company X targeted in a ransomware attack' do **not** reflect the reality. Most criminals take the opportunities presented to them, either through buying accesses that they deem likely profitable, or by scanning for a vulnerability in a product likely used in enterprise networks. There is far less return on investment for criminals to specifically target a single organisation. This is particularly true as the conversion rate from victim to payment is quite low. The vast majority of ransomware incidents are a result of large scale access gathering that is filtered later to identify those most likely to be suitable for ransomware.

Most ransomware incidents are not due to sophisticated attack techniques, but are usually the result of poor cyber hygiene. That's not to say that victims did not take cyber security seriously; modern IT estates are exceptionally complex, particularly for organisations that have undergone acquisitions and mergers, and security controls can be difficult to implement effectively across complex environments.

Poor cyber hygiene can include unpatched devices, poor password protection, or lack of multi-factor authentication (MFA). Remedying these are not silver bullets, but implementing such measures would interrupt the majority of ransomware attacks. MFA in particular is often not in place, which enables many ransomware attacks to be successful.

Direct exploitation

A common method for gathering initial accesses is to scan the internet for devices with known vulnerabilities. Some groups use commercial datasets for this such as Shodan, but many others conduct the scanning themselves, as it is not a difficult process to set up. Criminals look for devices that are likely to be in businesses (rather than home environments). Examples include Microsoft Exchange servers, platforms such as Citrix or VMware, VPN devices and firewall devices.

Figure 4 covers global volumes of Microsoft Exchange servers that are vulnerable and where the patches have been available from Microsoft since 15th February 2023. The graph shows minimal change in overall availability of exploitable devices over one month after the patch became available. This trend indicates that despite patches being available, they are not being consistently applied and there are still rich pickings for cyber criminals to use as an initial access.

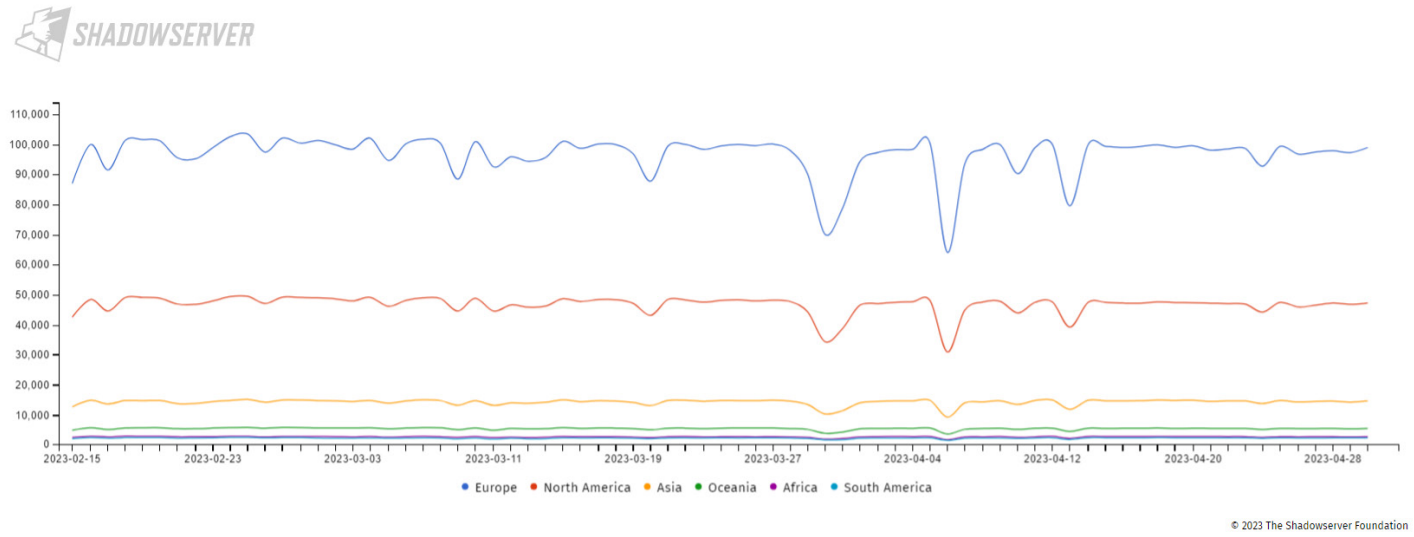


Figure 4. Shadowserver tracking of Microsoft Exchange exposure (Dashboard · The Shadowserver Foundation)[13]

Criminal use of exploits often surges shortly after certain critical patches are released indicating they are being reverse engineered from the patches. In most cases, an exploit is widely available in the criminal forums in less than one week from the patch being released.

A zero-day exploit is a recently discovered vulnerability, not yet known to vendors or antivirus companies, that criminals can exploit. Cyber criminals don't need to develop their own zero-day exploits as doing so is expensive, and there are many devices 'in the wild' that are not patched regularly. However, some actors have been known to use zero-day exploits, most notably there are public reports of Cl0p's use of the Accellion, GoAnywhere and MOVEit vulnerabilities. This would account for the large spike in Cl0p victims in Figure 1 in 2023. Actors conducting ransomware will buy exploit code from other criminals, or modify exploit code from GitHub.

Note:

The NCSC strongly recommends creating a vulnerability management[14] plan that prioritises vulnerabilities that are accessible from the internet. The list of exploits being used changes rapidly based on the availability of vulnerable systems and the introduction of new exploits to the market, so it is not enough to just patch those known to be in use currently.

Brute force access

As previously discussed, poor password practice is another common access vector for enabling ransomware. In the same way actors can scan for known vulnerable devices, it is equally straightforward to scan for a device type and test common passwords in brute force attacks. In some cases, default passwords (that are widely known and shared) have not been changed. Tools like Crowbar, Hydra and NLBrute, specifically designed for conducting brute force attacks, make it easy for malicious actors (who can also use the same approach with certain network perimeter devices and common services such as RDP or SSH) to gain access.

Malicious actors will also use passwords from previous database breaches to gain access to current systems, since password re-use is relatively common. There is a premium charged for fresh accesses from recent database breaches, since most breach databases are often older (and therefore less likely to work in ransomware attacks).

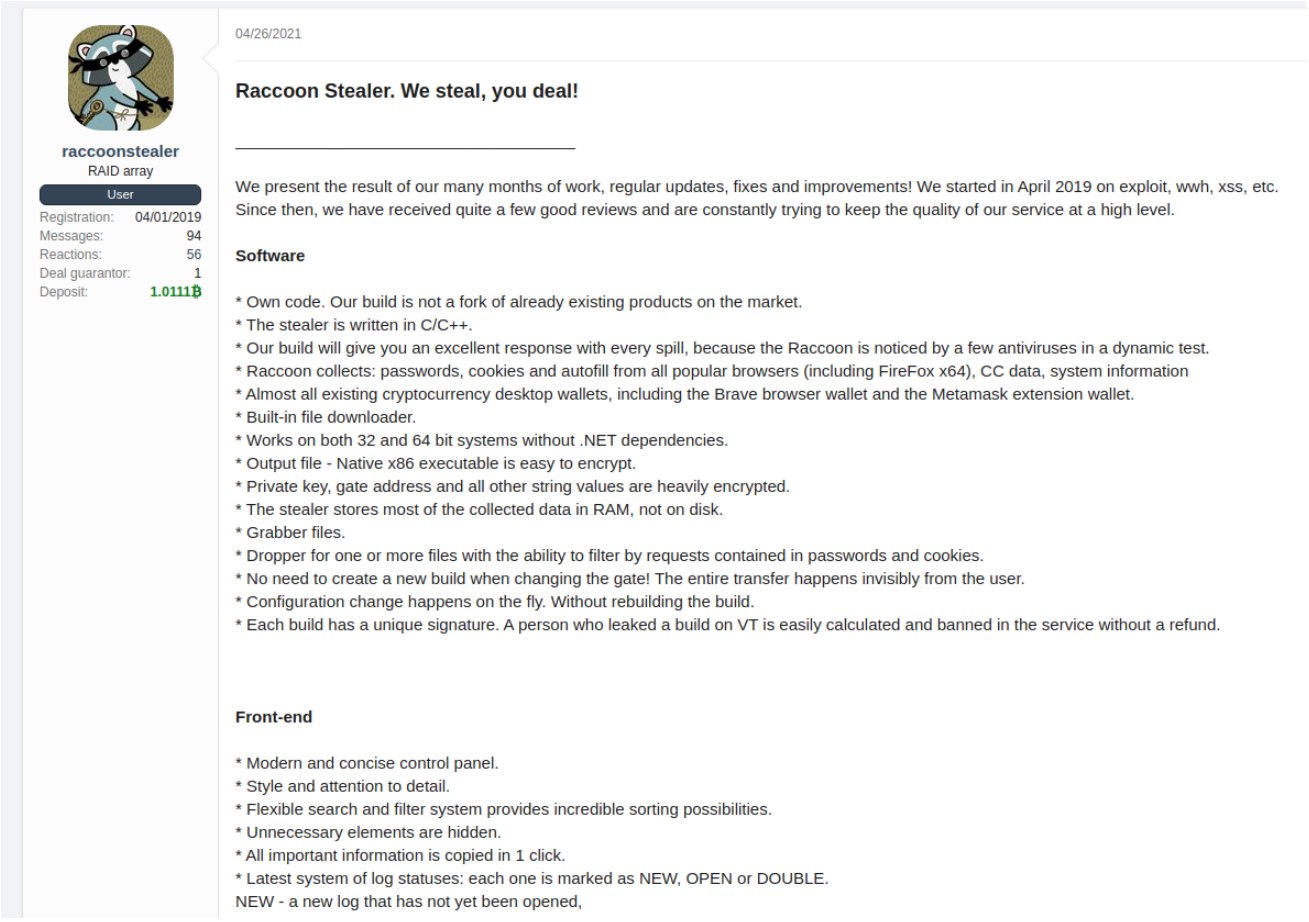
Stealers and loaders

'Stealers' are a type of malware available on criminal forums that are used to harvest a variety of useful information (including credentials) which other criminals can use in fraud and/or ransomware attacks. In some cases, versions of the stealers have been leaked onto GitHub making them widely available for anyone to use. Prices range from hundreds to thousands of US dollars per month.

Common features of stealers are:

- stealing passwords stored in web browsers
- stealing cookies, browser version and other configuration details
- stealing form entry data from web browsers
- stealing stored credit card details
- taking screenshots
- capturing antivirus details
- logging keyboard presses from users

This malware can evade detection by antivirus software due to the availability of criminal services that specialise in 'crypting' or modifying malware to ensure it's not detected.



raccoonstealer
RAID array
User
Registration: 04/01/2019
Messages: 94
Reactions: 56
Deal guarantor: 1
Deposit: 1.0111฿

04/26/2021

Raccoon Stealer. We steal, you deal!

We present the result of our many months of work, regular updates, fixes and improvements! We started in April 2019 on exploit, wwh, xss, etc. Since then, we have received quite a few good reviews and are constantly trying to keep the quality of our service at a high level.

Software

* Own code. Our build is not a fork of already existing products on the market.
* The stealer is written in C/C++.
* Our build will give you an excellent response with every spill, because the Raccoon is noticed by a few antiviruses in a dynamic test.
* Raccoon collects: passwords, cookies and autofill from all popular browsers (including FireFox x64), CC data, system information
* Almost all existing cryptocurrency desktop wallets, including the Brave browser wallet and the Metamask extension wallet.
* Built-in file downloader.
* Works on both 32 and 64 bit systems without .NET dependencies.
* Output file - Native x86 executable is easy to encrypt.
* Private key, gate address and all other string values are heavily encrypted.
* The stealer stores most of the collected data in RAM, not on disk.
* Grabber files.
* Dropper for one or more files with the ability to filter by requests contained in passwords and cookies.
* No need to create a new build when changing the gate! The entire transfer happens invisibly from the user.
* Configuration change happens on the fly. Without rebuilding the build.
* Each build has a unique signature. A person who leaked a build on VT is easily calculated and banned in the service without a refund.

Front-end

* Modern and concise control panel.
* Style and attention to detail.
* Flexible search and filter system provides incredible sorting possibilities.
* Unnecessary elements are hidden.
* All important information is copied in 1 click.
* Latest system of log statuses: each one is marked as NEW, OPEN or DOUBLE.
NEW - a new log that has not yet been opened,

Figure 5. Screenshot of Raccoon Stealer advertisement translated into English

Note:

Although the credential stealing malware described above is used to access passwords stored in web browsers, the NCSC's advice for general members of the public[15] remains to store credentials in web browsers. This prevents the majority of users from using easily-guessed passwords (or re-using the same passwords across multiple accounts), both of which put people at risk following large scale data leaks when online services are compromised.

'Loaders' are another type of malware used to gather basic system information which is then used to deploy other malware. Loaders can be used to determine if a system is viable for ransomware before deploying more capable malware (and spending the time necessary to take over the whole network).

We'll often see a blurring of functionality, with some loaders gaining stealer functionality, and some stealers operating as loaders. Loaders were more common at the start of the growth in ransomware, with loaders such as Emotet and Trickbot leading to large volumes of victims that actors could choose from. More recently they are less common, with stolen credentials and vulnerable devices being a more readily available access.

According to reporting in PWCs Strategic Intelligence Bulletin*, the most popular stealers on the market are RedLine Stealer, Raccoon Stealer and Vidar. Many criminals use these tools to steal credentials. Cyber crime marketplaces make it very easy for criminals to sell these stolen credentials in bulk. These marketplaces are similar to automated vending carts (AVCs) discussed in the previous NCSC cyber crime report, and allow criminals to buy credentials, typically under $100 for most services.

Genesis is one such marketplace that was subject to a law enforcement disruption[16] and prior to the disruption was among the top 3 reported credential marketplaces. Genesis also provided browser cookies and fingerprints so actors can mimic the original device and bypass authentication checks. These stolen credentials are preferred to large breach databases, as they are more recent and used by fewer criminals, and so more likely to work. Stealers are increasingly used outside the corporate environment due to the increase in home working and bring your own device (BYOD) initiatives. The availability of credentials for sale has been increasing as illustrated in the diagram below:

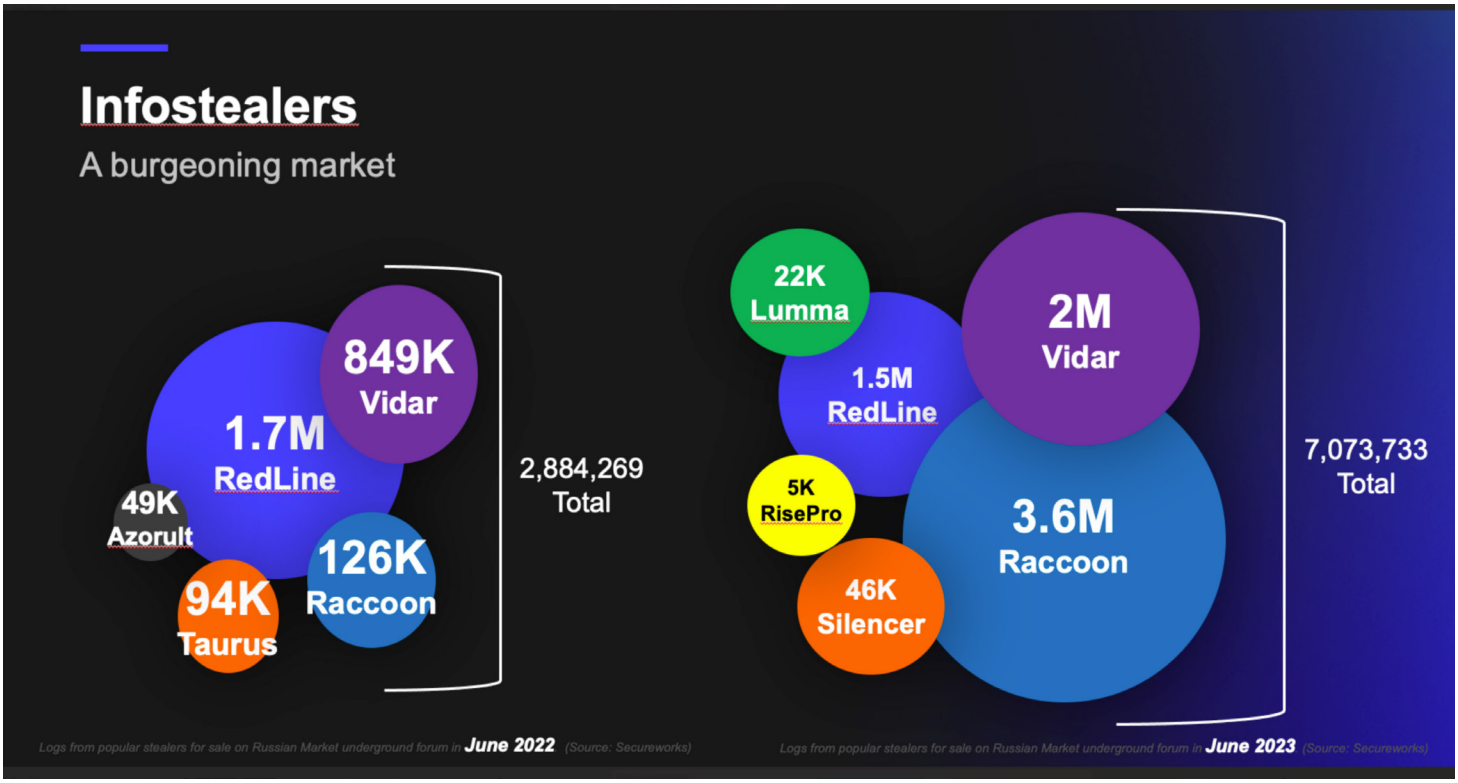


Figure 6. Approximate credential availability on Russian Market criminal forum 2022 vs 2023. Source: Secureworks

The deployment of MFA on remotely accessible business accounts makes this much harder for criminals, but there are - at a cost - services that use social engineering techniques to bypass these mitigations.

** CTO-SIB-20230224-01A - Strategic Intelligence Bulletin: We can steal it for you wholesale", Price Waterhouse Coopers, 2023*

Distribution

Loaders and stealers require distribution to gain large victim volumes. Phishing services on criminal forums supply this distribution by sending a large number of emails with malicious attachments, or links to trick users into visiting malicious websites.

Other popular distribution techniques include:

- malvertising (when an attacker uses advertising as a delivery method for malicious activity)
- SEO (search engine optimisation) poisoning to return malicious links to common search terms
- embedding malware in cracked software

Traffic Distribution Systems (TDS) also play an important role in malware delivery. A TDS is similar to legitimate advertising services; they receive visits from users who have clicked links in malicious emails, and capture basic system information such as geographical location, browser or operating system version. The main benefit of a TDS is that it allows cyber criminals to define redirection rules from an administration panel based on the type of visitors browsing the system's web of malicious landing pages. This means that different categories of visitors can be redirected to different campaigns, depending on the target audience.

TDSs were very popular with exploit kits to ensure the correct exploits were used against the right browser to minimise the risk of detection. More recently they are proving very popular in phishing distribution, blocking known security research IPs from receiving the malicious payload for analysis.

Initial access brokers

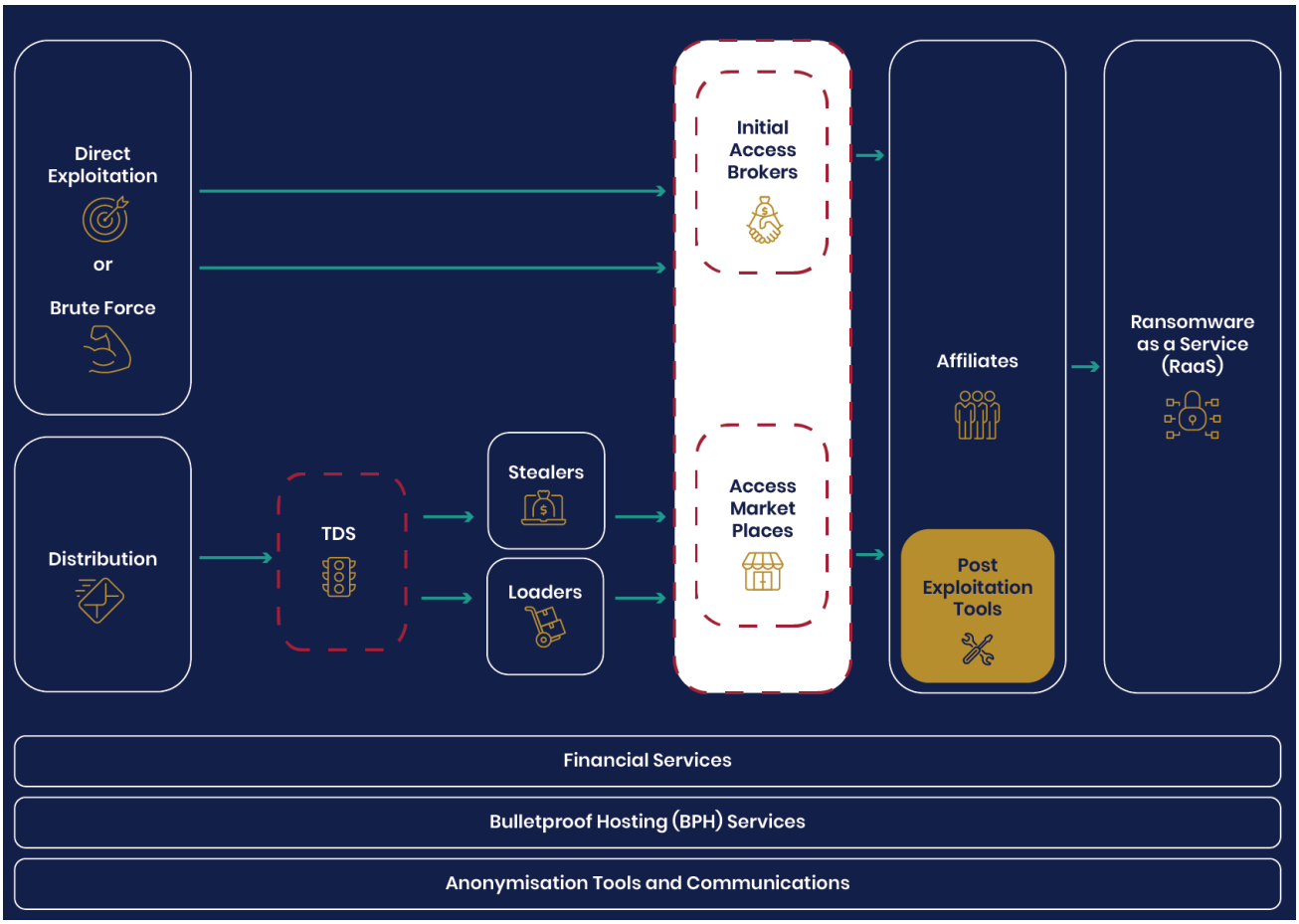


Figure 7. Initial access brokers

An alternative to selling credentials to marketplaces is to sell to Initial Access Brokers (IABs). IABs are actors that take in large volumes of access garnered across these access methods, and filter for the highest value victims to resell at a higher cost. They will often buy stolen credentials in bulk, or conduct their own scanning for vulnerable systems.

An IAB's primary function is to filter these for likely businesses, test the access works (occasionally setting up backup access methods) and triaging the business for onward sale. Some work to requirements from ransomware actors, others do not have specific customers in mind and just re-advertise the confirmed high value access for anyone to buy.

Once accesses have been validated, IABs will often confirm the access is to a corporate network, identify the approximate size of the network in terms of number of machines/users, as well as attempt to identify who the victim is from the network domain information. This is used to work out the value of the company from records such as Companies House and commercial datasets like ZoomInfo. IABs resell accesses for thousands of US Dollars depending on the value of the victim.

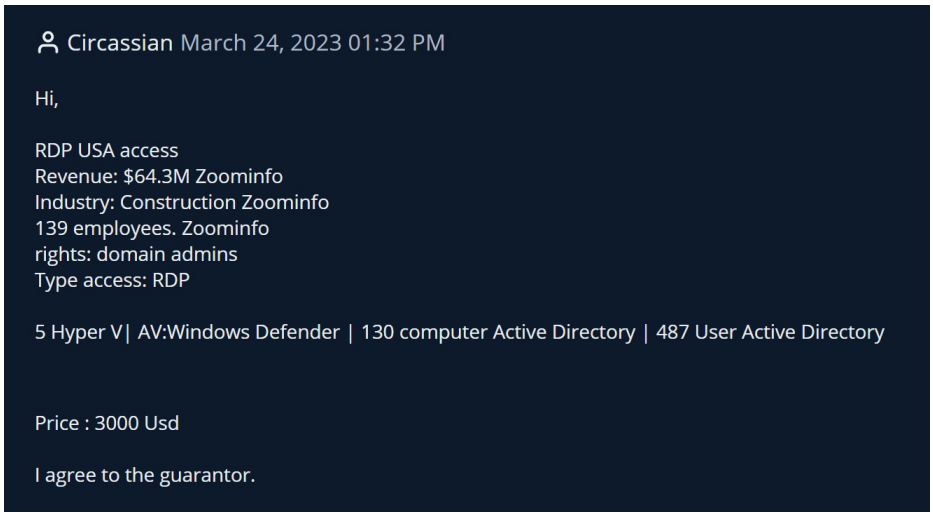


Figure 8. Copy of an IAB advertisement of an access for sale. Source: Mandiant

Ransomware business models

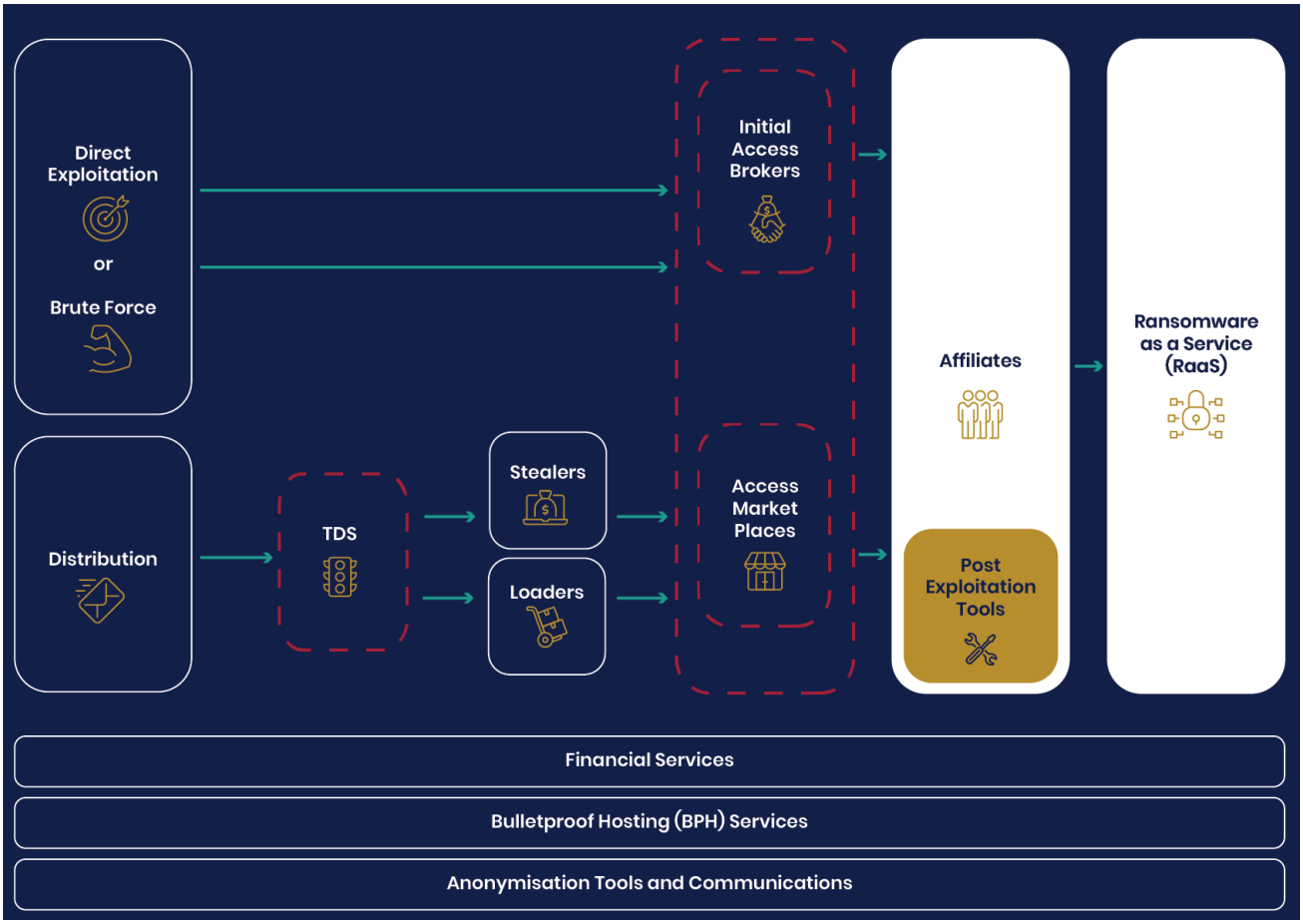
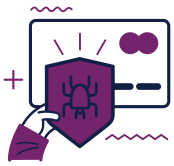


Figure 9. Ransomware business models

As with any business types, there are many business models to obtain ransomware. Each have their own quirks, and will often reflect the preferences of the actors running the business, and how they like to work.

Buy-a-build



Possibly the simplest business model available to ransomware actors is to obtain existing ransomware code. This is typically low cost, as writing ransomware is not technically challenging from a coding perspective. The sale of the Dharma ransomware source code was listed for as little as 2,000 US Dollars and many others have had their ransomware source code leaked to criminal forums, or even the public. Recent examples include LockBit 3.0 and Conti, both of which can now be used by any actor.

The buy-a-build model tends to appeal most to the smaller groups with lower skill levels who are less likely to pull in large ransoms from big businesses. They also often lack the connections to operate in the other business models that are more profitable.

Perhaps counter-intuitively, the leaking of ransomware source code is **not** particularly helpful for security professionals. While criminals and independent researchers leaking code in this fashion undermines the original criminals who wrote it, the impact is rarely sustained as it is easy to start again and rebrand. Furthermore, it diversifies the ransomware available as they are used by multiple actors or built into new "Frankenstein ransomware" variants, making attribution of attacks to actors even harder for law enforcement.

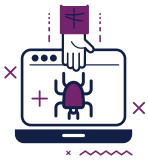
In-house

The traditional ransomware business model is a full 'in-house' solution, where the same threat group responsible for developing the ransomware conduct much of the attack. That is not to say they do not require the marketplace, in fact many still use it for parts of the attack chain, including for cryptocurrency services.

The group behind Conti ransomware predominantly followed this model. While they recruited operators (affiliates), the payment model was very different to ransomware as a service. Since the group provided most of the accesses, the tooling and operating procedures (as well as the ransomware itself), the group held onto the majority of the profits. Most of the operators are understood to have been salaried and took a commission from the ransomware payments with the rest going to the core group. This is largely reflective of car sales models in legitimate businesses, where the salesperson receives a base salary (and annual leave, and suchlike) but is encouraged to make more sales through the use of commission.

While this model is less common, some groups still primarily operate as an in-house business model. Ransomware such as Cuba and Vice Society are not available for sale in the criminal marketplaces. In the case of Cuba ransomware, access was primarily via the Hancitor Loader. Vice Society typically do not use loaders, and are routinely observed conducting attacks against the education sector. Use of a common access vector or targeting profile suggests it is a single group conducting these operations from the point of access to the deployment of ransomware. Access vectors and other behaviours are much more diverse in 'ransomware as a service' models.

Ransomware as a Service (RaaS)



The ransomware business model seen most frequently is 'ransomware as a service' (RaaS). In this model, ransomware groups typically provide a web portal to enable affiliates/customers to customise their ransomware and obtain new builds with unique encryption keys per customer. Many include a communications platform to make the ransom negotiation easier and more anonymous for the affiliate. Most ransomware will also include features to delete local backups to hinder recovery. Other features of the service include access to data leak sites, where affiliates can publish stolen data as an added incentive for victims to pay.

RaaS groups are often aware of western laws and regulations and use that knowledge to shape their criminal activity. Data leak sites became popular in the hope of pressuring victims that could face large fines under laws such as UK GDPR and the Data Protection Act 2018[17]. While the threat of leaking sensitive data (whether intellectual property or personal data) often carries real weight with victims, the victim can be liable for not protecting the data, regardless of whether it becomes public on the leak site.

A recent example of this can be found in the reported negotiations between Lockbit and the Royal Mail[18], where the malicious actor attempts to use this leverage, failing to grasp that the very public nature of the attack (and that LockBit publicly claimed the attack) means that paying to prevent the data release does not necessarily prevent the victim being fined for the breach. They could have paid an exorbitant cost to the criminals, and still be subject to GDPR regulations and potentially be fined. The relationship between RaaS group and affiliate can further be observed in the reporting around this incident, as LockBit initially denied responsibility until the group identified which affiliate conducted the attack.

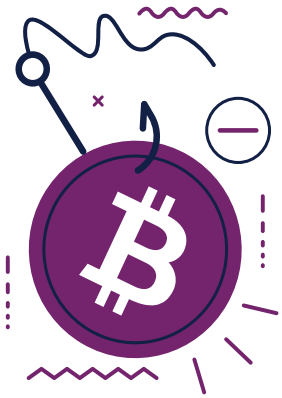
There are many subtle differences between the RaaS groups as each attempts to refine their business models for maximum profit. Some will deploy ransomware attacks on businesses dependent on IT systems (such as manufacturing and logistics) but conduct data leak-only attacks (with no encryption) against sectors where the data privacy is more important, such as law firms or healthcare services.

The most important thing to note about RaaS is that typically it's the **affiliate** that obtains and uses the access, **not** the RaaS group. This is an important distinction in the eyes of the law and is actually two different offences under the Computer Misuse Act (CMA) (1990). Writing and selling ransomware falls under Section 3A of the CMA, while the affiliate conducting the attack is subject to Section 3 or 3ZA (depending on the impact).

One example of this is the attack on Royal Mail, which was publicly attributed to LockBit. However, LockBit are simply the RaaS group who are said to have provided the ransomware, it would have been a LockBit affiliate that obtained and exploited the access. While many RaaS groups have 'terms of service' that prevent affiliates ransoming certain targets (such as healthcare and critical national infrastructure) the enforcement of it is varied between groups. In some cases they 'vet' the victim before supplying the ransomware. In others it is retrospectively applied, and may mean they won't supply to the affiliate for use in future attacks. In either scenario, the control the RaaS group exerts over the affiliate is often *after* the point of compromise.

The enforcement of the terms of service reflect a risk-driven approach to the attention RaaS groups invite from UK and international law enforcement. Law enforcement activity can reduce the popularity of a criminal service, with affiliates switching to other brands. This was seen with DarkSide ransomware that the FBI has said was used in the attack on the US Colonial Pipeline[19], resulting in widespread disruption to the US east coast. The Darkside ransomware collapsed as a brand after law enforcement seized the cryptocurrency of the affiliate that conducted the attack.

In recognition of the increased skillset of the affiliate (and the fact they do a larger portion of the work), the RaaS group typically takes a smaller percentage of the ransom. Until recently this was approximately 45%, but with the increased competition from more RaaS groups, that figure has decreased.



Ransomware affiliates

RaaS is the only ransomware business model that uses affiliates to deploy the ransomware, but they are such a critical component of the system that they deserve their own section in this paper.

The term 'ransomware affiliates' refers to the threat actors conducting the 'hand-on-keyboard' attacks after the initial access, up to the point of deploying ransomware. Affiliates are the glue in the system; they buy accesses from IABs, buy ransomware from RaaS groups, and put everything together to conduct a devastating attack on a business. It is the affiliate that chooses which accesses to buy (or which accesses to use if garnering their own accesses) and they choose which RaaS service they want to use.

The advantages an affiliate gains from using RaaS is primarily anonymity. By purchasing a ransomware that many other affiliates are using (and also using the same communications platform for engaging victims), it is much harder to attribute an affiliate to an attack. From the outside it appears that the RaaS group conducted the attack. However, the 'anonymity' is not total; the RaaS group must track the affiliates behind each attack in order to sort the payments. In addition, there is often enough identifying information in which tools are used (and how they are deployed and the order they are used in) to cluster and attribute attacks to the same affiliate.

Post exploitation tools

Post exploitation tools are primarily used by affiliates. They are often tools that are built for system administrators or legitimate adversary simulation teams to enable improvement of system security. They are a challenge for security professionals as they are legitimate tools and are widely available, so they can't simply be banned/disrupted wholesale in the same way that malware can.

The most popular of these tools is Cobalt Strike. Other tools include Meterpreter, Sliver and Brute Ratel. To evade detection, criminals are also using existing administration tools and free trials of legitimate remote management software, such as Atera and Splashtop. Many criminals are not experts in conducting attacks, and groups will also sell accesses to those actors who don't have the skills to use the tools effectively.

Financial services

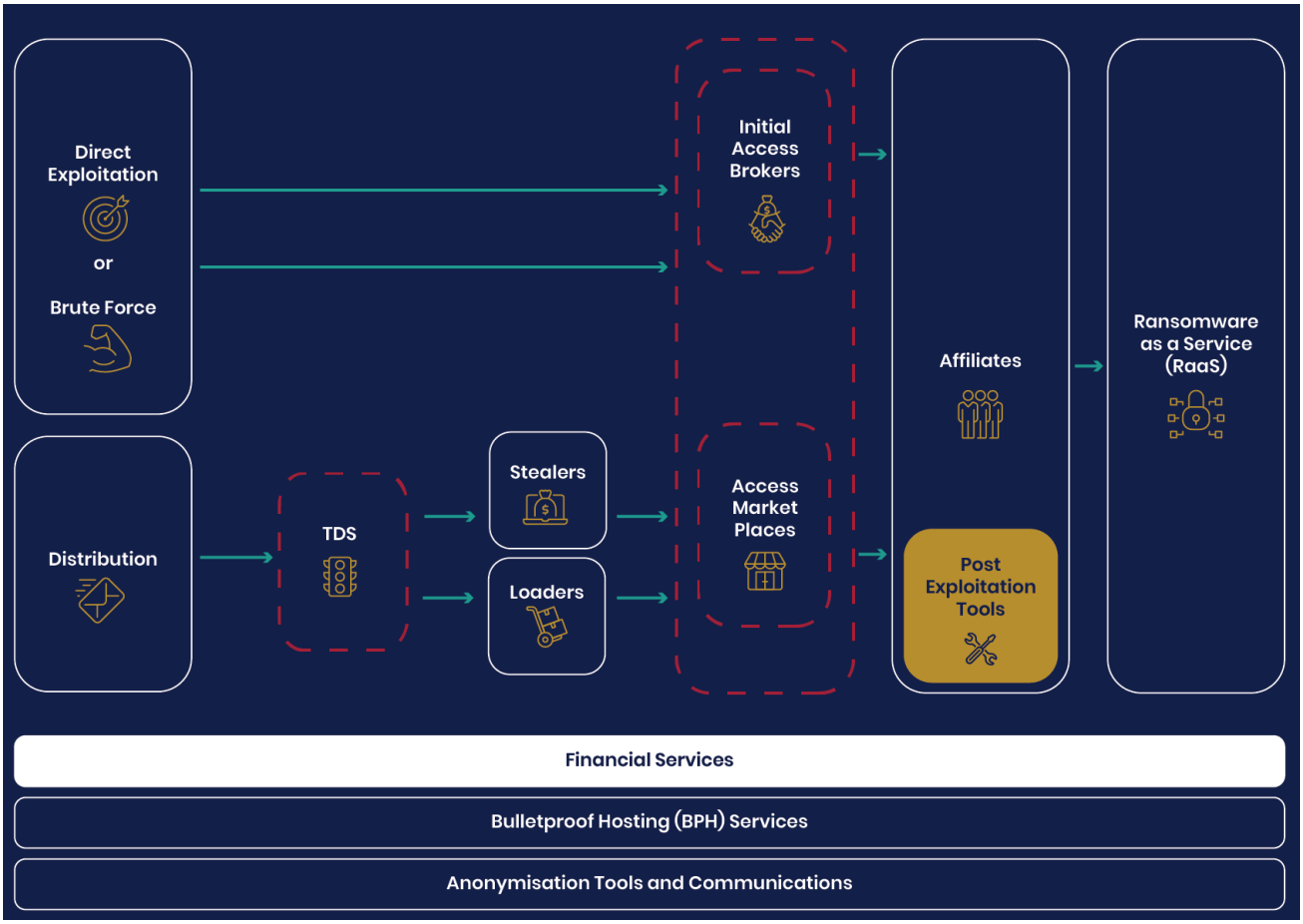


Figure 10. Financial services

Finally, if the victim makes a payment following an attack, the criminals need to convert the cryptocurrency to hard currency to spend. There are many services that can 'tumble' cryptocurrency through several exchanges, splitting the payment into smaller transactions to make funds more difficult to trace.

Although some exchanges are legitimate, there are also several cryptocurrency exchanges that are complicit in assisting ransomware criminals to exchange cryptocurrency into other forms of currency. Examples of this includes SUEX, which has been sanctioned by the US Department of Treasury[20].

Cryptocurrency is a staple of ransomware and the criminals rely upon the anonymity it provides. A lack of funds can quickly dismantle criminal enterprises as was seen with the group behind Conti. Analysis of the leaked chat data showed that the actor in charge of the group appeared to leave in late January to early February 2022 (a month prior to the leaks) and took with them the majority of the money to pay wages. As a result, communications were sent to the wider group enforcing a temporary disbanding due to lack of funds.

The NCA demonstrated that a cryptowallet associated with the actor in charge of the criminal group behind Conti contained approximately 95m US Dollars at the time the actor left Conti, however the remaining actors could no longer pay wages to the actors conducting the work. Arrest videos released by Russian authorities of cyber criminal actors typically show small, untidy apartments and a rather unglamorous lifestyle. This shows that while those at the top can accumulate large amounts of wealth and live extravagant lifestyles, the majority of criminals don't make the profits that likely tempted them to the business in the first place.

Conclusion

This white paper has illustrated how ransomware and extortion attacks reflect a diverse and varied business model that's reliant on a complex supply chain. Focussing on specific ransomware strains can be confusing at best, and unhelpful at worst. Most ransomware incidents are **not** due to sophisticated attack techniques; the initial accesses to victims are gained opportunistically, with success usually the result of poor cyber hygiene. Implementing the NCSC guidance listed below would interrupt the majority of attacks.

The shifts in the ecosystem around ransomware and extortion demonstrate how cyber criminals will adopt whichever technology (or business model) allows them to best exploit their victims. This means the threat will continue to adapt and evolve as threat actors seek to maximise profits.

While on the surface, an attack can be attributed to a piece of ransomware (such as Lockbit), the reality is more nuanced, with a number of cyber criminal actors involved throughout the process. Tackling individual ransomware variants – something which the NCSC and NCA are frequently challenged on – is akin to treating the symptoms of an illness, and is of limited use unless the underlying disease is addressed. Taking a more holistic view by understanding the elements of the wider ecosystem allows us to better target the threat actors further upstream, in addition to playing 'whack-a-mole' with the ransomware groups.

Prevent and protect against ransomware

The following NCSC publications have been created to help organisations to defend themselves from ransomware, and to recover from the impact if they do suffer an attack.

NCSC guide to ransomware[21]
An area of the NCSC's website dedicated to ransomware.

Mitigating malware and ransomware attacks[22]
How to defend organisations against malware or ransomware attacks.

Protecting bulk personal data[23]
15 good practice measures for the protection of bulk data held by digital services.

Incident management[24]
How to effectively detect, respond to and resolve cyber incidents.

Multi-factor authentication for online services[25]
Advice for organisations on implementing multi-factor authentication (or 2-step verification).

All links

Foreword

1. **NCSC's Cyber Essentials programme:** https://www.ncsc.gov.uk/cyberessentials/overview
2. **The NCSC's ransomware pages:** https://www.ncsc.gov.uk/ransomware/home
3. **National Strategic Assessment 2023:** https://www.nationalcrimeagency.gov.uk/nsa
4. **Cyber Choices campaigns:** https://www.nationalcrimeagency.gov.uk/cyber-choices
5. **7 Russian ransomware criminals associated with the Conti-Trickbot group in February 2023:** https://www.gov.uk/government/news/uk-cracks-down-on-ransomware-actors

Introduction

6. **Ransomware attack on the Health Service Executive of Ireland:** https://www.bbc.co.uk/news/world-europe-57184977
7. **Colonial Pipeline in Texas:** https://www.bbc.co.uk/news/technology-57063636
8. **Multiple organisations in the education sector:** https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector
9. **Ransomware threat has evolved:** https://www.ncsc.gov.uk/blog-post/rise-of-ransomware

The evolution of ransomware

10. **Paying the ransom quickly doesn't always help:** https://www.ncsc.gov.uk/blog-post/why-more-transparency-around-cyber-attacks-is-a-good-thing-for-everyone

The cyber crime ecosystem

11. **EvilCorp:** https://www.bbc.co.uk/news/world-us-canada-50677512
12. **Conti:** https://www.bbc.co.uk/news/technology-64586361

Direct exploitation

13. **Dashboard: The Shadowserver Foundation:** https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=other&d1=2023-02-15&d2=2023-04-30&source=exchange&source=exchange6&group_by=geo&style=overlap
14. **Vulnerability management:** https://www.ncsc.gov.uk/guidance/vulnerability-management

Stealers and loaders

15. **NCSC's advice for general members of the public:** https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
16. **Law enforcement disruption:** https://www.bbc.co.uk/news/uk-65180488

Ransomware as a Service

17. **UK GDPR and the Data Protection Act 2018:** https://www.gov.uk/data-protection
18. **Lockbit and the Royal Mail:** https://www.bbc.co.uk/news/business-64718824
19. **The attack on the US Colonial Pipeline:** https://www.fbi.gov/news/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

Financial services

20. **SUEX, which has been sanctioned by the US Department of Treasury:** https://home.treasury.gov/news/press-releases/jy0364

Prevent and protect against ransomware

21. **NCSC's guide to ransomware:** https://www.ncsc.gov.uk/ransomware/home
22. **Mitigating malware and ransomware attacks:** https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
23. **Protecting bulk personal data:** https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data
24. **Incident management:** https://www.ncsc.gov.uk/collection/incident-management
25. **Multi-factor authentication for online services:** https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C113965