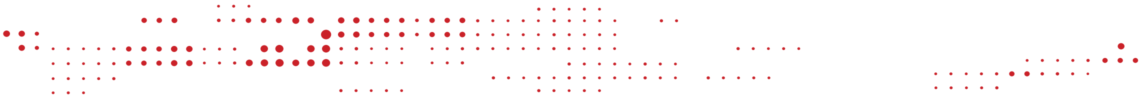
How to protect your IT environment against the

EVOLVING THREAT OF CYBER-CRIME

An investigation into the causes and effects of malicious data breaches as well as how to address them.

A PAPER BY REDSTOR | FEBRUARY 2018 | WWW.REDSTOR.COM



St James' Wharf | 99–105 Kings Road | Reading | Berkshire | RG1 3DD
t +44 (0)118 951 5200 | **e** sales@redstor.com | www.redstor.com
twitter.com/redstor linkedin.com/company/redstor

INTRODUCTION

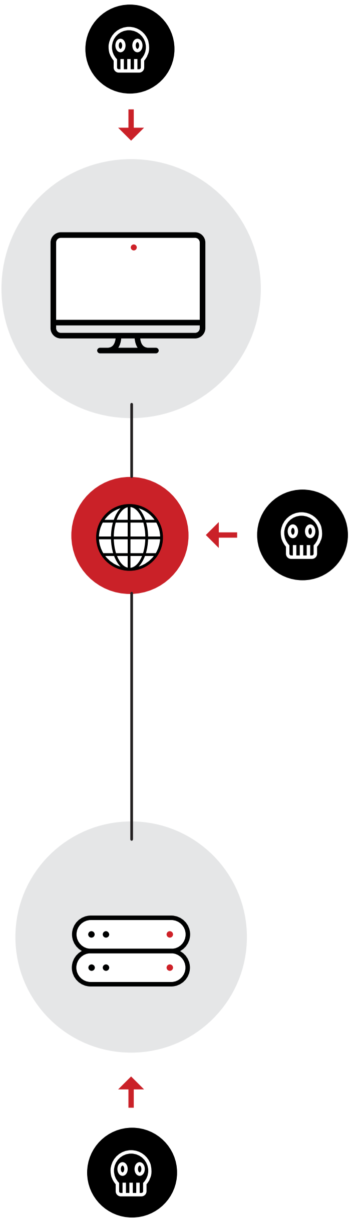
Malicious data breaches are making headline news on an almost weekly basis, and given the explosion of technology and data seen in recent years it is no wonder the ‘dark-side of tech’ is also on the rise. Cyber-criminals are well funded, well organised and money driven[1]; having successfully extorted ransom payments of millions it is very unlikely they are going to stop anytime soon.

Organisations and individuals alike are often lacking the knowledge to understand how and why their IT systems may be targeted. This attitude towards technology and cyber-security will have to change if there is any hope of stopping these kinds of attacks.

This paper will investigate the causes and effects of malicious data breaches and other types of cyber-attacks. It will also serve as an informative overview of the different types of cyber-attacks and some of the ways to reduce the threat they pose as well as how to recover from them.

WHAT IS CYBER-CRIME

> *“Cyber-crime is simply any criminal activity that occurs by means of computers or the internet’*



There are many different cyber-attacks that the cunning cyber-criminal can employ with differing effects, some designed to disrupt and some designed to extort for profit. Cyber-attacks are often well thought-out and carefully planned, with several stages to an attack, the first of which is often a ‘disarming’ of security protocols. Although sophisticated attacks will use multiple methods to attack a network, with varying success, most attacks can be identified to one category of attack. Some of the most common are:

- **Malware strains**
- **Phishing attacks**
- **Worms**
- **Denial of Service (DoS) attacks**

See Appendix A for definitions of types of cyber-attack

THE GROWING THREAT OF CYBER-CRIME

2016 was described as the year of Ransomware, due to a notable rise of attacks and the profiles of those companies who were being targeted. Hackers and other cyber criminals have vast resources available and are able to target hundreds if not thousands of devices, people and organisations at once. Wide-spread use of email combined with a lack of knowledge leads to many people infecting themselves to the gain of cyber-criminals.

Attacks have also been making headlines as a single attack or strain of malicious code is able to effect so many; a reported 300,000 organisations in the WannaCry attack. The number of those affected is not the only aspect that has increased. With criminals looking for a payday the sums being demanded for the safe return of data has increased. Reports of ransoms of up to $1 million have been reported and some organisations have felt they have had no choice but to pay up.

The National Cyber Security Centre (NCSC) and the National Crime Agency (NCA) among other security agencies have advised against paying ransoms.

Why are attacks increasing?

Cyber-attacks are increasing, in both severity and volume. Cyber-criminals are adapting to keep attacks effective, testing their software against scanning services that don't share the results with anti-virus vendors to avoid detection and building in code that causes malware to self-destruct if malware analysis software is detected on a system. They're also repeat targeting systems that have already been hit as well as infecting new systems, on a constant basis to increase the effectiveness of attacks.

The most obvious reason for a rise in the number of attacks is that being a cyber-criminal can, with relative ease, be very lucrative. Ransoms of around £300, paid in bitcoin, are common and are relatively likely to be paid, however much larger ransoms have been reported. These ransom payments can be in the thousands and in some cases even millions of pounds.

Although sophisticated cyber-attacks will take large amounts of time and planning to execute, many attacks are relatively easy to carry out. With much of the coding needed, available to buy on the dark-web, cyber-criminals can simply subscribe to a malware code service or repurpose code to create their own strain of malware and quickly distribute it. As so many attacks rely on an unsuspecting user taking an action, the easiest and most effective way to distribute them is via email. This means that individuals or organisations can be mass targeted by cyber-criminals, with one vital piece of information (an email address).

Why you shouldn't pay a ransom

It is advised by many regulatory authorities and experts that if you suffer a ransomware attack, that you should not pay the ransom. Cyber-criminals are fuelled by successfully extorting money from victims, paying a ransom directly attributes to this and could still leave you vulnerable. Paying a ransom once means that you are likely to do it again and cyber-criminals will know this, making them more likely to retarget paying victims.

Paying a ransom may seem like the quickest way to get data back and to cut out downtime, however, paying a ransom does not guarantee that you will get your data back. Data may not be unencrypted at all or may be corrupted, some ransomware strains have even been found to simply delete data rather than unencrypt it.

If best practice is being followed within an organisation, then a full copy of data will have been taken as a backup. This backup should be held securely off-site and therefore be unaffected by any ransomware attack. Restoring from a backup is the only way to guarantee all data is securely recovered and that cyber-criminals do not gain anything from encrypting systems.

While a cyber-criminal could generate and target random email addresses, it is more likely that a quick shopping spree on the dark web would wield better results. Email addresses are the piece of data most commonly stolen during a data breach and this gives cyber-criminals new targets. The Yahoo data breach in 2013 was initially touted to have contained around half a billion email addresses, 4-years later this number was revealed to have been 3-billion. That's 3-billion targets for cyber-criminals to try and extort.

With so many attacks taking place, why are law enforcement agencies not more effective in tracing cyber-criminals and stopping attacks? One reason is the rise of cryptocurrencies like bitcoin.

> *“Cryptocurrency is a digital currency or medium of exchange which is created and stored electronically in a blockchain. Encryption is used to both create the currency units as well as verify the transfer of funds. Cryptocurrency is largely anonymous. The reason for this is there is no central bank or authority and the network is completely decentralised. This makes it impossible to counterfeit and very difficult to trace. Cryptocurrency is also relatively immune to government interference or manipulation.*

As the use of cryptocurrencies has increased, cyber-criminals have realised they can use it to anonymously profit without the risk of being traced, unlike traditional money transfers.

HEADLINE ATTACKS

WannaCry

The WannaCry ransomware strain made headlines in March 2017 as the attack quickly took down networks spread across the globe. Companies affected by the attack included Renault, Deutsche Bahn, FedEx and Telefonica to name a few. The attack exploited a known vulnerability in Microsoft operating systems, for which a patch had been released, but many organisations clearly hadn't updated software to ensure its protection. In the 3-day period that the attack was active, a reported 300,000 organisations were affected over 150 countries.

> *"We've never seen something on this scale and that's because the ransomware itself has been combined with a worm application that allows the infection from one computer to quickly spread across other networks. That's why we're seeing these numbers increasing all the time and right across different sectors, right across the world."*

Rob Wainwright, Director of Europol

Lights out in the Ukraine

A few days before Christmas 2016, a region in the Ukraine fell victim to a cyber-attack[2] when hackers remotely shut down part of the power grid, leaving almost a quarter of a million people with no power. The hack, which gave the criminals access, was the result of months of planning and involved a phishing scam of emails[3] designed to look like they had come from friends and colleagues, to obtain passwords. Microsoft Word documents attached to the emails installed malware once opened, the malware known as BlackEnergy 3 gathered passwords and logins. After several months of work, cyber-criminals then had all of the credentials necessary to remotely log in to systems and cut power at 17 sub-stations. The hackers simultaneously jammed company phone lines and rewrote firmware to ensure the blackout could not be reversed remotely, engineers had to manually reset systems to bring power back.

Equifax left out of credit

Credit giant, Equifax, suffered a large-scale data breach affecting customers across the globe and resulting in the swift departure of CEO Richard Smith. The initial statement from the company confirmed that an estimated 143 million customers had had data stolen in the states alone, this number has since risen. Hackers were able to exploit a known security flaw in a software package heavily utilised by the organisation; a patch had been released, however Equifax had failed to identify systems that needed to have the patch applied. Hackers had access to systems from mid-May to July and the company made no announcement until September for fears of more attacks.

THE EVOLUTION OF CYBER-ATTACKS

Traditional antivirus solutions are constantly being developed and improved to ensure that the latest cyber-threats are being protected against. Software developers will similarly update versions with new patches and fixes to ensure that there are no exploitable vulnerabilities in their software. Cyber-criminals therefore face an increasingly difficult task to find routes into systems.

However, the nature of cyber-attacks is changing, this can be seen by the sheer scale of attacks making headlines, how much data is being stolen and how large ransom demands are becoming. A common effort to increase the ability and effectiveness of an attack is to combine different strains of code. The WannaCry attack was unprecedented in scale and the speed at which it spread due to this.

WannaCry utilised an NSA originating exploit that was leaked by the Shadow Brokers hacking collective in mid-April. The exploit in question, codenamed EternalBlue, targets a vulnerability found in Server Message Block (SMB) code built into all modern versions of Windows. The exploit provides a means of remotely commandeering computers running Windows. This vulnerability is present on any Windows version from XP through Server 2012. By incorporating the EternalBlue exploit with a self-replicating[4] payload, WannaCry can spread itself in "worm" fashion from vulnerable machine to vulnerable machine across the network. The result is that after an initial infection, there is no need for emails to be opened or links to be clicked, the virus silently spreads itself without the need for human interaction.

The GoldenEye strain of ransomware that was seen shortly after the WannaCry attack featured two layers of encryption. While ransomware has always targeted files and encrypted them to stop a user being able to use their computers, GoldenEye encrypted both the files and file structures known as NTFS structures, this stopped files from being accessed, even in their encrypted format.

Cyber-attacks often require an element of human intervention to work, whether someone accessing a malicious file or falling victim to a phishing scam and giving away log in information. The evolution of cyber-attacks is unlikely to see this change in many cases and for large well planned out attacks, it is usually vital.

CYBER-CRIME AND THE INTERNET OF THINGS (IOT)

The technology industry, with the help of the internet, is rapidly evolving and innovative products and solutions are becoming available to organisations and individuals across the globe. The Internet of Things (IoT) is an area that is looking to bring innovation to users by connecting new and existing mediums and making more items 'smart'. However, with new technologies comes a new threat as cyber-criminals and hackers quickly look for security flaws to exploit. 'Smart' cars may look like the future but should the control of those vehicles fall into the wrong hands it could cause chaos.

IoT has built a bad name for itself when it comes to security and has become known for poor levels of security and regular hacks. Hackers have quickly worked out how to turn connected devices into botnets that can be used to launch large scale attacks on other organisations and networks, often without knowledge of the IoT device owner. In 2016, hackers successfully created a botnet including over 150,000 IoT devices and initiated an attack with global repercussions [5]. The problem stemmed from poor credential management; the Mirai strain of malware used in the attack took advantage of default passwords and account settings on IoT devices and with relative ease was able access and control the devices.

HOW TO PROTECT AGAINST CYBER-ATTACKS

Protecting data against the effects of a cyber-attack can be difficult[6]; attacks are growing in complexity and volume and they can strike at any time. However, there are principles that can be implemented in any situation or by any organisation that can work in favour of a potential victim, reducing the chance of being hit by a cyber-attack and limiting the impact in the event of an attack. Many industry bodies and regulators will also recommend their own processes for mitigating risk and ensuring protection.

Governance and Procedures

Internal governance is a crucial factor in beginning to protect against cyber-threats. While it can be difficult to completely remove the risk of a cyber-attack, it can be quite easy to reduce risk and to mitigate some of the potential damage. Across industries, authoritative bodies will have regulations that must be abided by, on top of state-driven legislation and data laws.

Implementing internal policies and procedures to cover management of all aspects of digital and technical resource ensures that an organisation has a set of standards to uphold and security levels to continually build upon. In the event of a cyber-attack, it also provides a benchmark to test against and could enable an organisation to work out where a breach stemmed from.

Risk Assessment

Assessing risk should be an ongoing process within any organisation, especially given the rate of change within the cyber-threat landscape. Software and services should always be kept up to date to benefit from the latest protection elements from vendors who regularly patch software to protect against known threats. Some organisations will regularly employ ethical hackers to do penetration testing and understand where a threat could come from; if any areas of weakness are found, they can then be improved upon and protected against

> *“At Redstor, we regularly role play risk scenarios to identify weaknesses in our systems and processes, with a view to constantly improving them.*
>
> *My advice is to ask technicians from different teams what could put you out of business, don’t shy away from uncomfortable conversations like insider threats. Assess which are most harmful and likely to occur, then walk through the most pressing risks identified and work out how they might be eliminated or at least minimised.*
>
> *When doing this exercise, what I’ve found most surprising is not how many risks exist but often how many opportunities there are to mitigate them.”*

Thomas Campbell, Technical Services Director, Redstor

Staff Training

Human error or intervention is often the first step in a data breach or cyber-attack, as poorly trained staff are often not aware of what to look out for or how to protect their own systems. As seen in the WannaCry attack, malicious codes can be combined with ‘worm’ programmes so an infection can spread from one machine to infect an entire network. Making staff more aware of what cyber-threats they face and what they may look like is a great starting point for any organisation and will add a layer of protection that anti-virus programmes can’t. By tailoring training to be specific across different roles within an organisation, it is likely to be more effective.

Managing Access to Systems

The effectiveness of a cyber-attack can be partially limited to how much of a network can be accessed and what data is stored on that network. Only too often, cyber-criminals have had the opportunity to steel vast amounts of data by gaining access to systems that should have been isolated from the wider network. By tiering access to systems and keeping separate networks within an organisation, security can be increased and an infection from a single machine won’t affect the entire organisation.

Importantly, regulators such as the Information Commissioners Office (ICO), will always investigate how access was gained to systems and what could have been done to mitigate the risk[7]. This will have a direct effect on the penalties and fines that an organisation may face.

> *“Cyber security should be of concern to all in this digital age. Like it or not, our lives are dependent upon a myriad of computer based services, both social and commercial. Most of these rely on information exchange and that information can be sensitive. Recent high-profile events are testimony to the global reach of cyber-attacks and the pervasiveness of their impact; who would have thought that hackers from across the world could prevent surgical procedures from occurring in the UK! As individuals, groups and organisations we protect what is valuable to us and that must include digital data. We need to be aware of the risks of exposing information to exploitation and increasingly, those dangers concern denial of access as much as third party intrusion.*
>
> *There are numerous approaches to securing data but perhaps the most effective means of protecting against loss is offsite backup. Having a copy held remotely in isolation from the source means that recovery is possible from the worst-case scenario - total loss of the original data. Even better, if that copy can be made available online, then it is accessible whenever and wherever it is needed.”*

Paul Esson, Senior Technical Consultant, Redstor

Managing Vendors

As is highlighted in the upcoming General Data Protection Regulation (GDPR), the access that vendors (Data processors) have, has an effect on the integrity of data. Working with compliant vendors and vendors who have secure cyber policies will be increasingly important going forward. Internal actions to increase security can be completely negated by giving the wrong vendor access to systems, only for them to fall into the wrong hands and result in a cyber-attack or data breach.

ACTIONS TO TAKE

Whatever your level of protection, there are actions and policies that can be implemented to reduce the threat of an attack and reduce the damage potential of an attack. These policies should become part of core practices within the organisation, helping to ensure they are carried out correctly by all staff.

Anti-virus

Anti-virus is one of the most established forms of defence against cyber-attacks and can protect against a host of threats in real-time. Anti-virus solutions should be in place across your entire network and regularly monitored to ensure that they are up to date and working. Anti-virus vendors will release software updates and update definitions on an on-going basis to protect against new strains and types of attack.

Implement a patching schedule

In a similar vein to anti-virus definitions being regularly updated, software providers will release patches and software updates to protect against new threats and vulnerabilities in systems. By systematically scheduling patching updates across devices and machines on a network, you can ensure that the software and firmware is up to date and that your network is protected.

Isolate guest networks

Having multiple networks within an organisation is vital to mitigating risk and stopping infections spreading from one system to the next. Implementing an isolated guest Wi-Fi network will ensure that any infection introduced to a network will only have an effect on a cub-set of systems. It's very difficult to control what guests access but it is possible to limit any damage that could be done.

Removable media policy

Infections can be easily spread via removable media. Policies should be put into place around the use of removable media to limit its use and ensure sensitive data is not at risk. If more secure alternatives are available these should be considered; one alternative would be to use a secure cloud sharing platform.

Password guidance

The number of attacks focused on gaining passwords is growing and it is becoming increasingly common that gaining passwords to administrator accounts is the first step in a sophisticated attack. It is important not to use generic passwords or passwords that can be easily guessed as these leave systems vulnerable. Enabling two-factor authentication where it can be used will improve security and mitigate the risk of a password hack attack[8].

DR / BC planning to recover from an attack

Disaster recovery planning aims to help an organisation deal with a large-scale outage and get back to operational capacity quickly. The threat of cyber-attack now means that planning for a disaster must include the possibility of this disaster having been a cyber-attack. The plan should give an overview of which data is most critical and should be recovered first, how this will be done and also include who needs to be contacted. Working with suppliers and vendors who have a proven track record of dealing with DR scenarios can be vital to this process.

CONCLUSION

Cyber-crime is clearly a threat to organisations of all sizes and one that is quickly changing and evolving to stay ahead of traditional protection techniques such as anti-virus. While the introduction of new technologies has positive effects on the way many organisations work, they also present new challenges in protection and new opportunities for cyber-criminals to attempt to breach a network.

To begin protecting against cyber-crime it is important to gain a clear understanding of what the threats are; many organisations are unaware of the threats and therefore how to protect against them. With an understanding of what cyber-crimes are and what they may mean to you, you can quickly start to assess the risk and understand how to begin protecting your organisation.

It is important to review where you are starting and to regularly risk assess systems that are in use. Cyber-criminals are well-funded and fluid in the way that they attack, often staging attacks over months and using different entry points to gain an advantage over security systems. Protecting against cyber-crimes is not a one-off solution and requires an ongoing investment of time. Without monitoring systems, it is impossible to know if they are protected and it can be almost impossible to understand if a cyber-attack has taken place, if it’s not ransomware, as many hacks will be silent.

Technology trends have seen an increase in both the number of threats and the damage that can be done by them, cyber-attacks are evolving and the cyber-security industry needs to do the same.

APPENDIX A

Cyber-attacks and what they mean

Malware

Malware is any type of malicious software that is often distributed via an active download, email or as a result of systems being unintentionally open to vulnerabilities. Commonly known types of Malware include Ransomware, Worms, Virus Attacks and Trojans.

Ransomware

Ransomware is one of the most well-known types of cyber-crime today, due in part to its rapid growth in volume through-out 2016. Although ransomware attacks, which encrypt a user's data or systems and demand a ransom payment for its return, have been around for several years, it is only recently that cyber-criminals have really cashed in and begun mass targeting people on a global scale to extort payments. Among those who have made the news having been hit, are hospitals, charities and schools; it is reported that some ransom payments have demanded up to $1million.

Worms

Worms have been around a very long time but today are lesser known attacks although still common. worm is a self-replicating programme that will attack a system until it finds a vulnerability, once the vulnerability is found it will traverse a network and continue looking for further vulnerabilities, often reporting back all vulnerable machines and systems as it goes.

Virus Attacks and Trojans

Virus attacks are another established kind of malware and have been common place for years. Anti-virus software is usually be able to identify and stop a virus before it is able to infect a system this is not always the case, especially if a virus is very new and has not yet been identified 'in the wild' and added to a list of known threats. Viruses can do considerable damage and are often designed to wipe out data or access to systems rather than simply to hold it to ransom or extort an organisation. A trojan is a type of virus that hides itself in the form of a seemingly helpful or harmless programme. Trojans can be less likely to be caught by anti-virus programmes as they require an active download and execution from the user.

Phishing

A phishing attack is usually stage one of a multi-stage attack as it is used to gather information such as account details, email addresses or passwords. A phishing attack is usually indiscriminately distributed by email, is designed to appear as if sent from a legitimate sender and will often link through to an illegitimate site requesting the entry of personal data. In recent years, we have seen the addition of 'spear-phishing' and 'whaling'. These terms refer to increasingly targeted methods of gathering more valuable information from specific information or high-profile targets with access to valuable information.

Password Hacking or Cracking

Password cracking has been around since passwords were invented and essentially refers to circumventing password protection. Typically, password cracking involves a hacker brute forcing their way into a system, repeatedly entering passwords until the correct one is found. Cracking is CPU intensive, therefore the more CPU power that can be assigned to the task, the faster a password will be cracked. Cracking has evolved over the years to cope with many security features designed to foil the ability of hackers to 'brute force' passwords such as 'captcha forms' and password form time-outs.

Denial of Service (DoS) Attacks

A DoS attack sees cyber-criminals sending high volumes of traffic to a network to overload the system so that it cannot operate. Disrupting a network could have the knock-on effect of halting security on the network or making it easier for hackers to access through other means. In recent years, Distributed Denial of Service (DDoS) attacks have become the norm. In this instance, the impact of the attack is amplified greatly by using numerous systems to launch an attack simultaneously. Often the systems used in the attack are part of a 'botnet' of systems controlled by the attacker remotely for nefarious purposes.

Other definitions

Cyber-crime

Cyber-crime is simply any criminal activity that occurs by means of computers or the internet.

Dark Web

The dark web is part of the world wide web that is only accessible using specialist software. This allows users as well as website operators to remain anonymous or untraceable. Transactions that take place on the dark web usually involve cryptocurrencies such as Bitcoin.

Crypto-currency

Cryptocurrency is a digital currency or medium of exchange which is created and stored electronically in a blockchain. Encryption is used to both create the currency units as well as verify the transfer of funds. Cryptocurrency is largely anonymous.

Bitcoin

Bitcoin is a specific type of Cryptocurrency popular on the dark web and with cyber-criminals looking to extort ransoms. This specific cryptocurrency was created around 2009 and the estimated value of all Bitcoin in circulation is more than $7 billion.

Self-Replicating Technology

A self-replicating technology refers to a technical mechanism that can autonomously reproduce itself using resources found in its environment. Common uses for self-replicating technologies in cyber-attacks are to help infections spread across systems, infecting new machines as they go.

APPENDIX B

References

[1] 2017 Data Breach Investigations Report 10th Edition – Source of information is publicly available, sign up required

[2] Could hackers turn out the lights? - http://www.bbc.co.uk/news/technology-35204921Security of IoT - https://www.redstor.com/news/security-iot

[3] Ukraine cyber-attacks 'could happen to UK'- http://www.bbc.co.uk/news/technology-35686493

[4] Self Replicating Machine - https://en.wikipedia.org/wiki/Self-replicating_machine

[5] Security of IoT - https://www.redstor.com/news/security-iot
Password guidance summary - https://www.ncsc.gov.uk/guidance/password-guidance-summary-how-protect-against-password-guessing-attacks

[6] Security Best Practices - https://www.symantec.com/page.jsp?id=stopping_malware

[7] ICO investigations - https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/08/council-fined-for-leaving-vulnerable-people-s-personal-information-exposed-online-for-five-years/

[8] Password guidance summary - https://www.ncsc.gov.uk/guidance/password-guidance-summary-how-protect-against-password-guessing-attacks

St James' Wharf | 99–105 Kings Road | Reading | Berkshire | RG1 3DD
t +44 (0)118 951 5200 | **e** sales@redstor.com | www.redstor.com
twitter.com/redstor linkedin.com/company/redstor