first response

Cybercrime in 2022

Introduction

This guide serves as a brief introduction to the cyber threat landscape in 2022 and to some of the potential threats to your organisation.

Cybercriminal activity is as varied as criminal activity in the physical domain. And as communication and information technology has developed over the last 20 years, cybercriminals have kept up with the pace, evolving into organised criminal networks.

Some of these networks are complete with recruitment teams, 24/7 support desks for ransom payments, software support, and development teams for malware. The distributed nature of the internet and the use of dark web allow criminal networks to operate outside of the jurisdiction of Western Law enforcement agencies.

Continued from previous page

To further complicate matters, IT networks and the way we use technology has changed significantly. It used to be easy to draw defences around your perimeter, your datacentre and server room. However, workforces are more distributed than ever and we are heavily reliant on the cloud.

Keeping on top of this change is difficult for IT teams, security teams and senior management.

Cyberattacks only need to be successful once for the attackers, and profits for successful attacks are significant. With ransom demands varying from £100K through to millions, and with business email compromise attacks being equally rewarding for would be attackers.

Cybercrime-as-a-service

Aided by the ability to maintain relative anonymity on the dark web and the ability to make lucrative and easy financial gains, the last few years has seen an explosion on the types of cybercriminal services available and the number of threat actors perpetrating them.

Cybercrime-as-a-service encompasses a number of different activities including the rental or sale of bespoke hacking tools, services and software, the sale of stolen network and user credentials from access brokers, the sale of zero-days (undisclosed critical system vulnerabilities and exploits), access to botnets (compromised internet-connected devices predominantly used for distributed-denial-of-service attacks, steal data, send spam and distribute malicious software), and pre-packaged ransomware kits.

It is a flourishing ecosystem of criminal activity which has evolved over the last ten years, with dedicated forums and marketplaces, further allowing threat actors to collaborate, organise and co-ordinate their activities.

Ransomware-as-a-service

Ransomware and large scale ransomware attacks have been featured regularly in the press over the last few years. Though ransomware-as-a-service may be a term unfamiliar to some, it is the rental or sale of ransomware by developers, and a commonly used business model available on cybercriminal markets. It provides access to ransomware kits and, and effectively allows those without much technical knowledge, to target and launch ransomware attacks for a commission.

This is a model which has become more popular over the last few years and has in parallel seen the wider network of criminal actors evolve the services they offer. With groups separating their operations into separate teams, units, affiliate groups, or partners, similar to how a modern enterprise would operate. This sees one team being responsible for recruitment of new affiliates, support of the software, one team responsible for negotiating ransom payments and communications with the victim, another for developing the ransomware kit, and others for providing access to the IT system of the victim. This allows operators to run efficient operations and to gain access to a wider pool of victims.

Continued from previous page

Expertise and skills various across the different teams with some being relative newbies and others being highly experienced having conducted multiple campaigns against targets. Threat actors will vary the types of attacks that they launch and different types of attacks will be used for different stages in campaign.

Credentials may be harvested through email spearphishing, where targets are lured to reveal their account names and passwords through social engineering and emails crafted to look like they're from official sources, alternatively they could look for vulnerabilities to exploit within an infrastructure. As of December 2021 there are nearly 300 common vulnerabilities that are actively exploited by ransomware groups.

Continued from previous page

Given the workload of IT and security teams, and with that the complexity of infrastructure and software, it is little surprise that threat actors are able to eventually exploit these vulnerabilities for their nefarious means. Vulnerabilities are discovered regularly and often vendors and IT teams are in a race against time to create patches and to roll them out across an infrastructure.

Threat actors will then use stolen credentials or vulnerabilities to gain a foothold within a system, moving across the environment, exfiltrating data, gathering sensitive information, and eventually launching a malicious payload which will often involve the encryption of core servers and services. Ultimately locking the organisation out of its own IT system, and shutting down the business operation. Without the encryption key, or reliable backups it is often impossible for the business to bring the systems back online. To add further insult to injury, the threat actors will then often threaten to leak corporate information unless the ransom is paid.

Distributed denial-of-service

DDoS attacks as they're more commonly known, are used to flood victims sites or services, typically web servers or network resources. The attack is usually only temporary but can cause significant damage and disruption, especially if they are conducted towards customer facing websites or web services, as they can cause those systems to become overloaded and unusable for the duration of the attack.

In 2021, we have seen the rise of triple extortion threats launched against ransomware victims, where attacks first compromise and encrypt a system, then threaten to leak confidential and sensitive data, then whilst the IT team and organisation are trying to recover, a third DDoS attack is launched to add further pressure on the victim to pay.

Access Brokers

Ransomware attacks are often broken down into separate stages, this means that threat actors don't need to be experts in every aspect of compromising the network, and also enables attacks to be launched more easily and effectively.

Access brokers specialise in gaining sensitive credentials for an organisation's environment, which are then resold on cybercriminal forums or through private channels. The value of credentials varies significantly depending on the type of credential, as well on the type and location of the organisation.

The shifting dynamics of remote work and technological advances has propelled our use of remote-access software, virtual private networks (VPNs) and other tools to enable us to work effectively whilst away from the office. Our reliance on this technology and the fact that software and systems developed by humans, are always vulnerable to potential flaws, provides access brokers with a wealth of opportunity to benefit from the weaknesses.

Phishing

Phishing is a type of cyberattack that uses email, SMS, phone or social media to entice a victim to share personal information, in the corporate domain phishing attacks are more likely to target account names or passwords.

Phishing kits are available to buy on the dark web and impersonate well known websites, often to good effect, once the victim is lured to the site they will then be prompted to enter their account name and password. These credentials can then be used against them, potentially to access internal resources, such as Microsoft 365 email or Sharepoint.

Once the attacker has the credential and access to internal resources, they can conduct research for additional targets within the organisation they may wish to gain access to, or even try to intercept payments and invoices to their own accounts. At this point a Business Email Compromise attack has taken place and individuals within the organisation may have been impersonated.

Continued from previous page

Alternatively, the phishing attempt may have been aiming to provoke the recipient to download a malicious file or piece of software onto their machine. Attackers have become adept at using new and novel techniques to ensure the files are downloaded and opened, carefully engineering their messages to bypass email security filters. If adequate controls aren't in place on the endpoint, once opened, the file will likely provide unauthorised access to the victim's machine and may have additional covert surveillance capability, such as keylogging, screen capture, or the ability to steal emails or chat logs.

This information and access can be used to gain further credentials for additional access within an environment, to steal data or sensitive information, or may even be used to compromise a third-party organisation, such as a supplier or customer.

Summary

Regardless of the size or type of organisation, the cyber threat landscape is a constantly changing one, with numerous different threats and threat actors.

It is a common misconception amongst small organisations to assume they won't be a target. This is not correct, in our experience smaller victims may be part of larger attack campaign to gain access to a larger upstream target, they may host or hold sensitive information (such as proprietary manufacturing process, or designs), they may be targeted as a cash rich organisation likely to pay a ransom or one making multiple financial transactions, or they may just be collateral damage from an inexperienced threat actor.

The last 10 years has seen the work environment change dramatically, this has been turbocharged by the development of global computing power, and disparate, interconnected, high-speed networks. Threat actors are no stranger to this revolution and use the disruption to benefit their own means.

This is a trend we expect to continue and because of the significant financial, operational and reputational damage that can be caused by a successful cyberattack, it is important that senior management teams engage with their IT team in implementing strong security practices and governance across the organisation.

About First Response

Established in 2013, First Response is a cybersecurity, digital forensics, and incident response company. Working with SMBs, SMEs & MSPs to protect their organisations and accelerate cybersecurity maturity. This is through outcome-focused consultancy and services incl. managed cybersecurity services (endpoint, network, mobile & cloud), and secure infrastructure design.

Our technical specialists comprise respected security and investigative professionals from a diverse set of backgrounds, including police cyber-crime units, the security services & enterprise network specialists.

We are headquartered in London with offices in Manchester and Rome, from where we assist our clients around the world. We also help organisations navigate the complex issues surrounding systems breaches, server compromises and data loss. Working with a wide variety of clients including banks, law firms, energy & manufacturing companies and public sector bodies.

first response

Contact

Email: info@first-response.co.uk
Tel: +44(0) 20 7193 4905
Web: https://first-response.co.uk/

first
response