K7 SECURITY

K7 Cyber Threat Monitor

MSME Report

FY 2021-22

www.k7computing.com

Contents

Foreword

"There are only two types of companies: Those that have been hacked and those that will be hacked."

– Robert S. Mueller III,
former Director of the FBI

Today, with the rapid changes in the cyber threat landscape, the cybersecurity industry at large acknowledges that there are only either companies that have been hacked or those that don't know they have been hacked.

In this day and age, cyber threats are very much a real and present danger to entities of all proportions: governments, multinational corporations, businesses of varying sizes, and all the way down to home users.

The Micro, Small, and Medium Enterprise (MSME) sector in India, like the human population, is second only to China, thereby playing an extremely crucial role in the country's economy. As a result, it is both good and bad news for anyone involved in an Indian MSME.

Good, obviously, because of the enormous growth potential, and evil because this is good news for cybercriminals.

Targeting MSMEs in the Indian sub-continent would be a no-brainer for cybercriminals as the attack surface, in terms of the number of potential victims, is enormous. Each attacker (or group of attackers) will run multiple campaigns using different techniques, tactics, and procedures (TTPs) at different times, with each new campaign being directed towards numerous targets simultaneously. Even if only a smattering of the attacks are successful, it would still ensure the attackers a good return on their investment.

This, coupled with the WFH scenario forced upon every business globally for the past couple of years due to the pandemic, has worsened things. Additionally, the threat actors' euphoria at seeing employees connecting to enterprise networks from personal devices (which are not controlled by their IT teams) using their home Wi-Fi (which most definitely are not behind firewalls and may not even be securely configured) would have made the threat actors elated as well.

Though specifically targeted attacks against a certain MSME are few and far between, there is enough empirical evidence to prove that more and more MSMEs are coming under attack.

The ramifications of such attacks on businesses could be multifold:

The economic cost of corporate and/or financial information theft; direct financial loss; trade disruption (including the inability to conduct online transactions for several days or weeks); and costs associated with restoring affected systems.

Reputational damage resulting in loss of customers and/or a drastic drop in sales, leading to a reduction in profits and impaired relationships with suppliers, partners, and other 3rd parties.

So, here are a couple of critical questions every MSME needs to give serious consideration:

First, how well informed do they feel about the risks of cybercrime?

And what is their overall level of preparedness against cyberattacks?

The MSMEs can quickly address the former by wading through several sites that provide information on the cyber threat landscape published by reliable sources, like the quarterly Cyber Threat Monitor reports from K7 Security.

The latter, however, requires a detailed study of the organization's entire network and the security tools currently implemented. This, followed up with the necessary diligence actions to tighten the loopholes identified by the survey, is key to ensuring the organization's assets are safe.

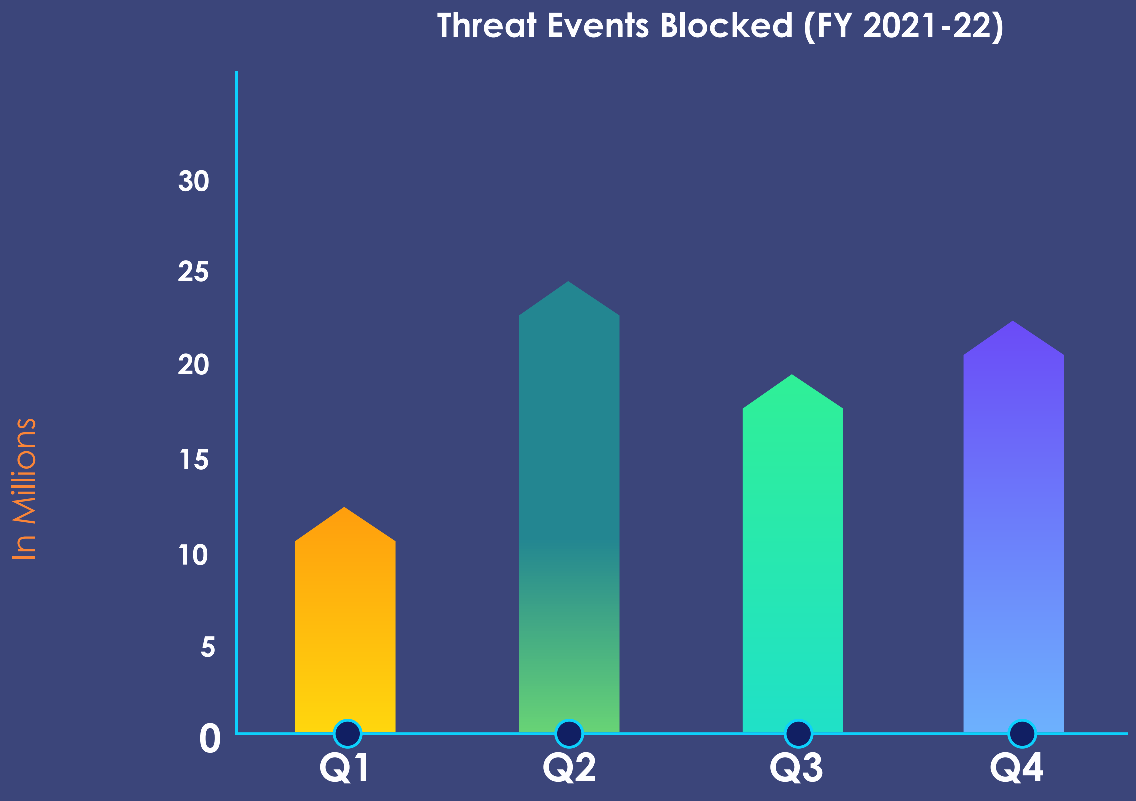
The MSME Threat Landscape

Apart from the size of the MSME sector, there are other reasons like smaller budgets and the size of the organizations in terms of the number of employees that lead to increasing attacks against the sector. Adversaries with different grades of sophistication catapult attacks on MSMEs, resulting in data breaches that lead to financial profits for the attackers.

Since most MSMEs have a smaller budget and fewer employees than large enterprises, they often lack a stringent security policy or a dedicated team to defend against the onslaught. As a result, they often get conned by the most common cyber attacks and lose vital assets such as customer records and intellectual property.

In the last financial year (April 2021 to March 2022), K7 Endpoint Security solutions blocked more than 78 million global threat events. And we saw more than a 100% spike in attacks between Q1 and Q2 of FY 2021-22.

What's worse, the increasing numbers also continued in the subsequent quarters.



Fallacies Versus Facts

Before even considering the areas that demand action, let us elucidate a few common fallacies surrounding the topic of cybersecurity in general.

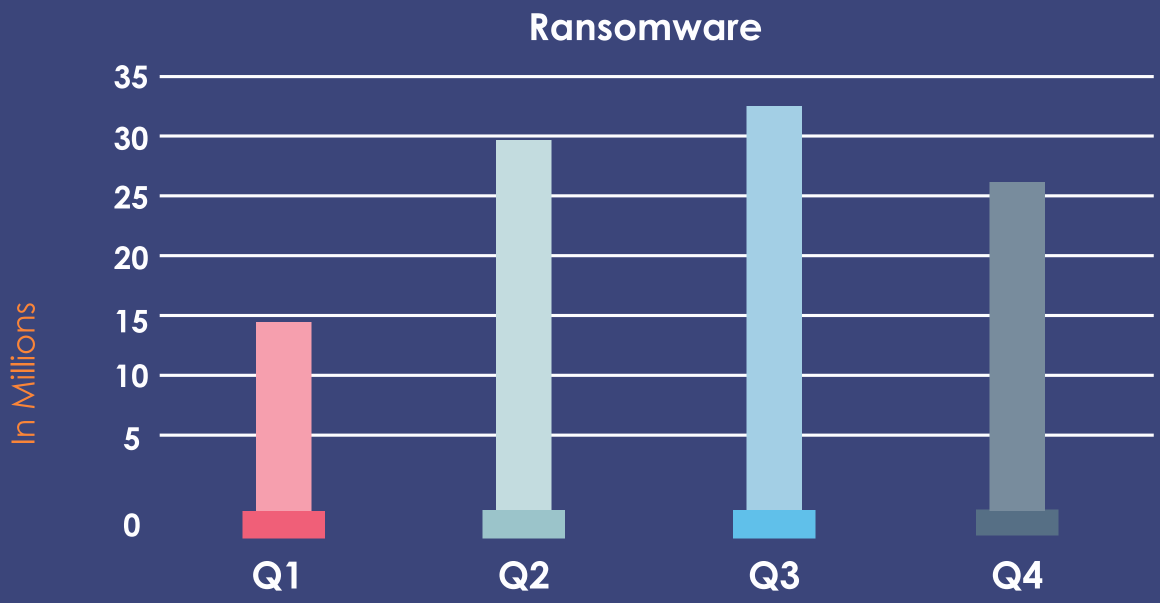
Fallacy	Fact
Cybercriminals do not target small and medium-sized businesses.	MSMEs have been a growing favorite of cyber criminals over the past several years, especially given the high possibility of small businesses not implementing advanced security solutions and the sheer volume of such companies.
An organization is cyber safe if it invests in sophisticated security tools.	While cybersecurity tools and solutions are essential to keep an organization safe from external attacks, their full capabilities can be harnessed only when they are appropriately configured, kept up-to-date, and their alerts and notifications are monitored and acted upon in a timely fashion.
Securing an organization's infrastructure is solely the responsibility of the IT team.	Cybersecurity breaches typically have long-lasting effects on an entire business. It is unrealistic for an IT team to shoulder this responsibility exclusively; it would need to be shared by every employee.
Compliance with industry regulations is adequate to keep a business cyber safe.	Adherence to industry regulations helps businesses have a smooth flow of operations, establishes trust, and avoids legal consequences, but does not go much beyond that as regulations, more often than not, lay down only the bare minimum of security practices rather than including the complete spectrum of cyber hygiene.
Secure internet-facing infrastructure is all you need to have.	This is again an imperative, but not enough; organizations need to have stringent security policies in place that are enforced in daily practice and give periodic awareness training to all their employees, lest they cause inadvertent damage like using infected USB devices on systems within the network.

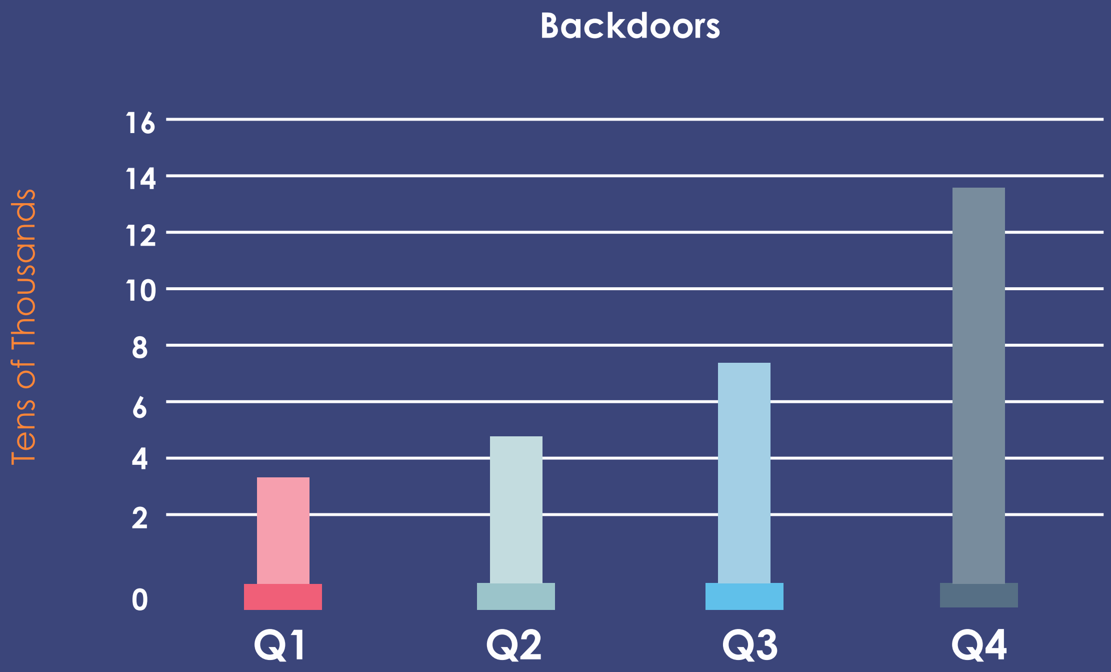
Attacks sprawled across the period

Putting a magnifying glass on the oncoming attacks, we see a large variety of outdated infrastructure and lack of cybersecurity strategy and cyber-hygiene practices among many other concerns.

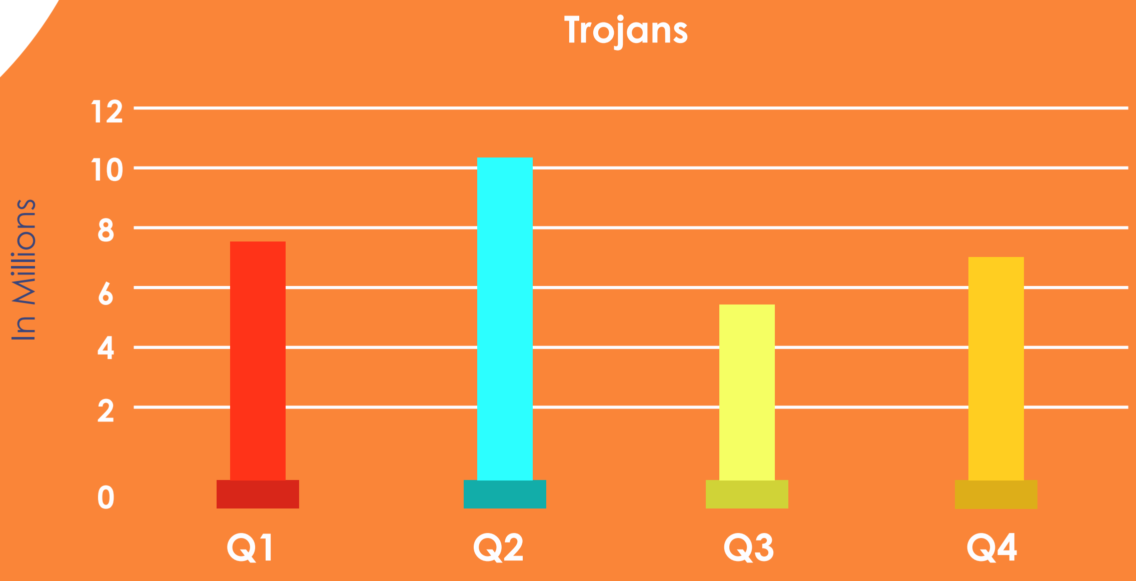
Unlike large organizations, MSMEs primarily focus on their existing assets to continue their business. As a result, over half of MSMEs have suffered at least one or more cyberattacks in the past financial year and the numbers are increasing every day.

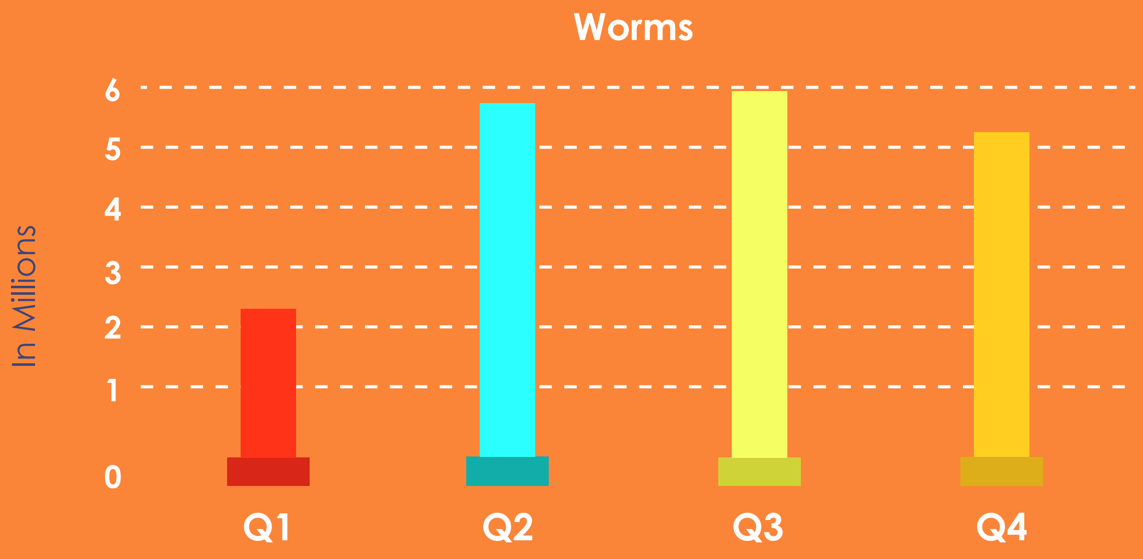
It is easily decipherable from the following graphical representations that, except for the Trojan category, the numbers of which have not spiked much over the last year, all the other malware categories have drastically increased.





◀◀ Back to contents





While the number of Trojan-based attacks stayed more or less the same for the last quarter, ransomware, worm, and backdoor-based attacks doubled, tripled, and quadrupled, respectively.

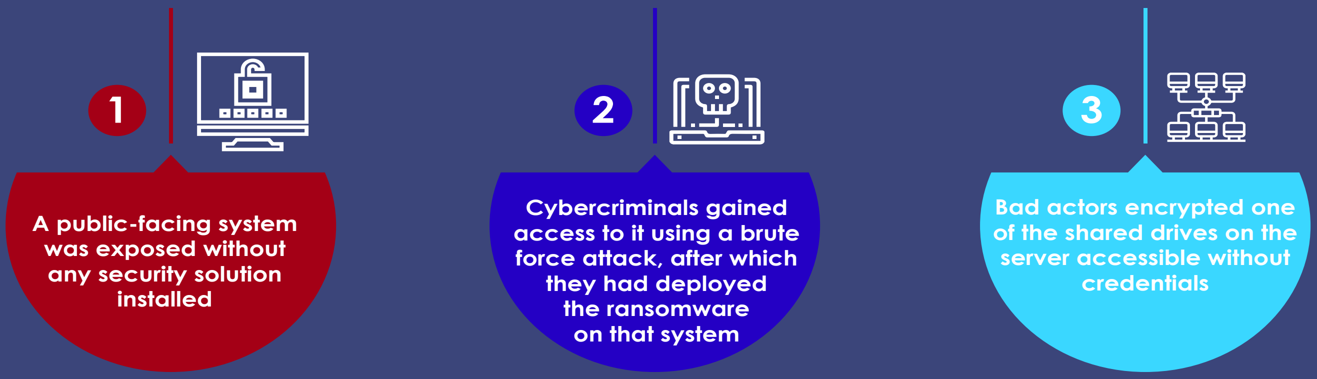
The results might be shocking to those who have not taken cybersecurity seriously. Still, they are (unfortunately) what is expected in light of the exponential digitalization of businesses across the country without the equivalent security measures in place.

To avoid the cyber-insecure list, businesses first need to identify the threat-prone parts of their present ecosystem. Assessing the flaws in your business network will be easier once you learn how modern attackers lure, intrude, and take control of business networks by looking at the security breaches owing to one or more of the abovementioned misconceptions.

◀◀ Back to contents

Case Study 1- The Ransomware Carnage

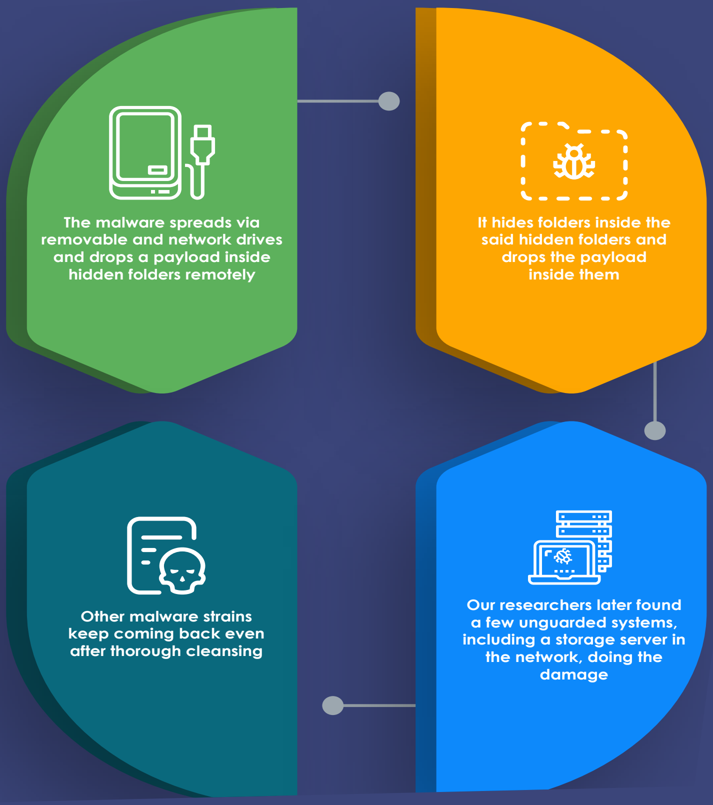
In yet another incident, an enterprise customer of ours reported a ransomware attack on one of their servers and one of the drives on the server was completely encrypted. Researchers from K7 Labs found the following chain of facts:



1. A public-facing system was exposed without any security solution installed
2. Cybercriminals gained access to it using a brute force attack, after which they had deployed the ransomware on that system
3. Bad actors encrypted one of the shared drives on the server accessible without credentials

Case Study 2 - Unprotected System Contaminating the Network

One of our enterprise customers recently reported that multiple folders were hidden on some of their systems. Even though the K7 solution installed on the infected systems detected and removed this worm, the issue kept recurring. The event prompted our researchers to study the network thoroughly, revealing that several systems on the customer's network, including one of their storage servers, did not have the K7 endpoint solution installed. On analysis, we found the following malicious actions on the network:



The malware spreads via removable and network drives and drops a payload inside hidden folders remotely

It hides folders inside the said hidden folders and drops the payload inside them

Our researchers later found a few unguarded systems, including a storage server in the network, doing the damage

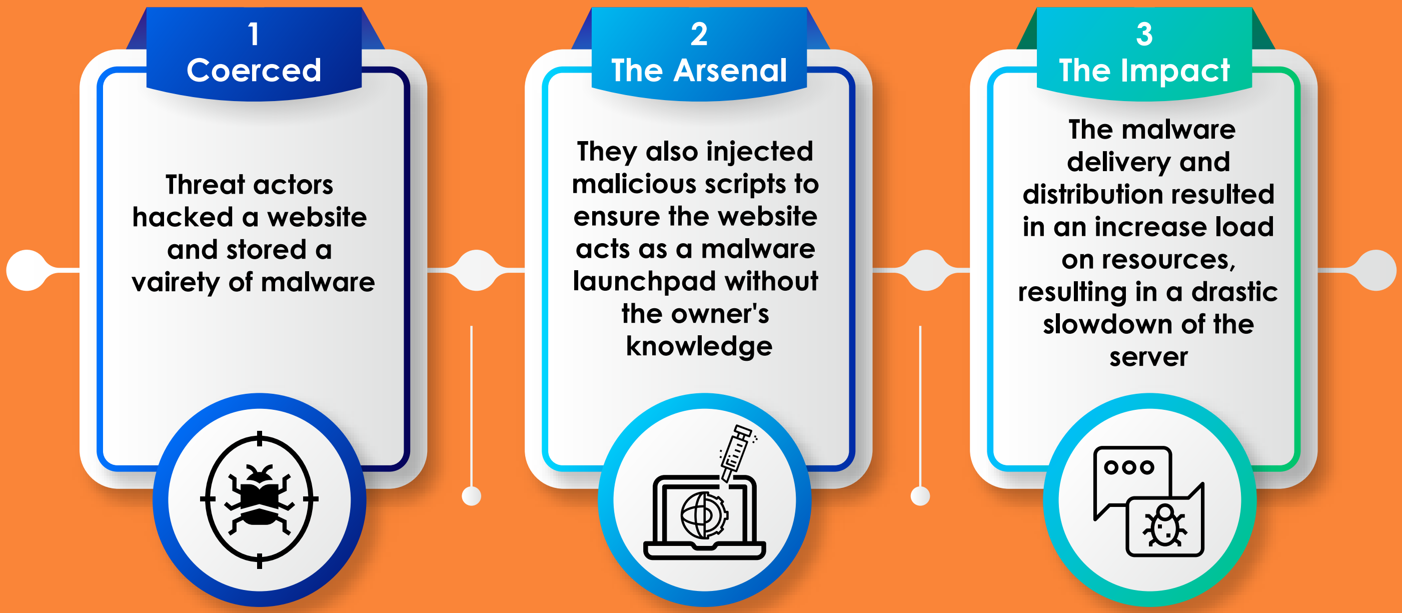
Other malware strains keep coming back even after thorough cleansing

◀◀ Back to contents

Case Study 3 - Compromised Website Exploited as a Malware Launchpad

K7 Lab received a request earlier this year from an institution that was not one of our customers. They stated they had many users complaining that some of their website pages were either not accessible or not loading correctly, and they wanted help to resolve this at the earliest.

Their description of the problem suggested Denial of Service (DoS) attacks on their web server.



1 Coerced

Threat actors hacked a website and stored a vairety of malware

2 The Arsenal

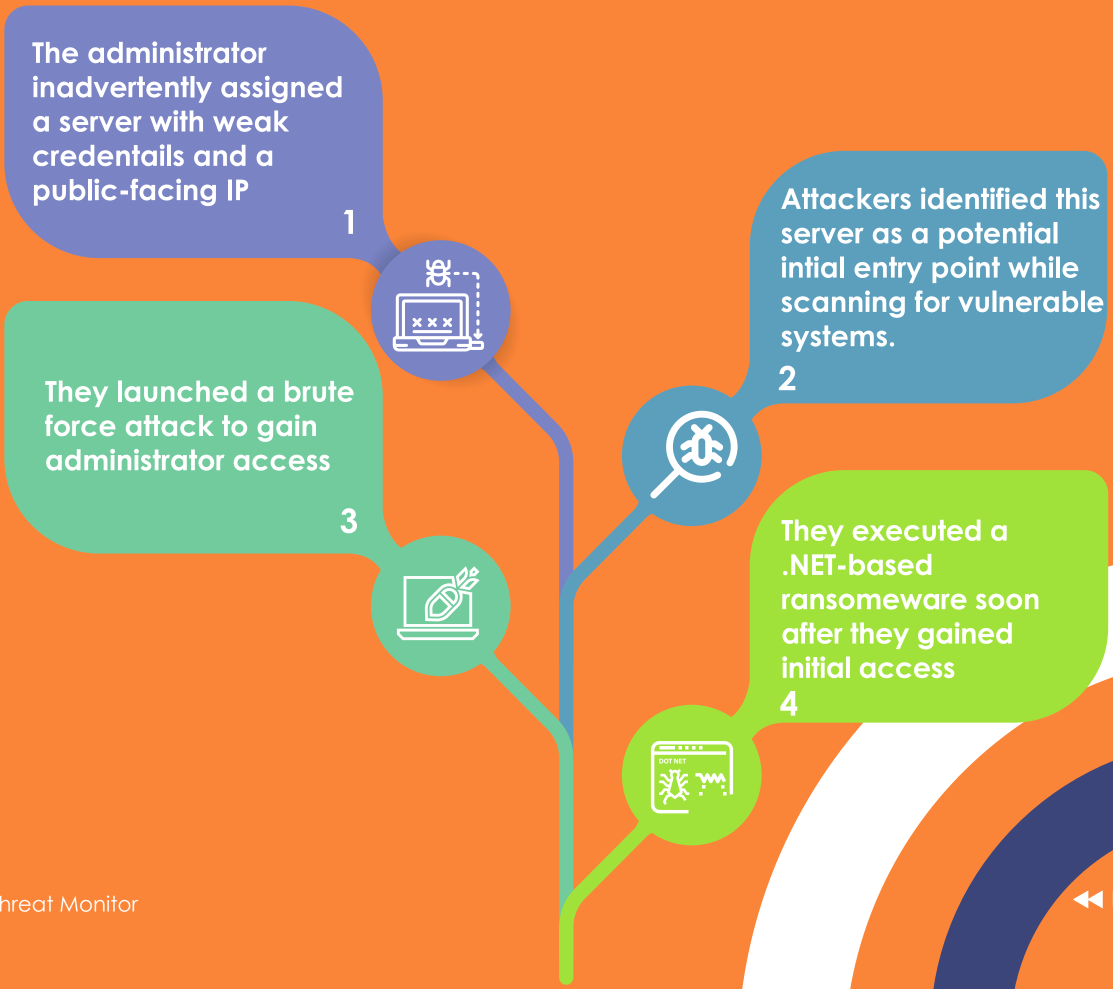
They also injected malicious scripts to ensure the website acts as a malware launchpad without the owner's knowledge

3 The Impact

The malware delivery and distribution resulted in an increase load on resources, resulting in a drastic slowdown of the server

Case Study 4 - Rogue Server Spawns Ransomware Attack

Another unfortunate but interesting incident was a ransomware attack caused by a server with weak credentials. Here is how it happened.



The administrator inadvertently assigned a server with weak credentails and a public-facing IP 1

Attackers identified this server as a potential intial entry point while scanning for vulnerable systems. 2

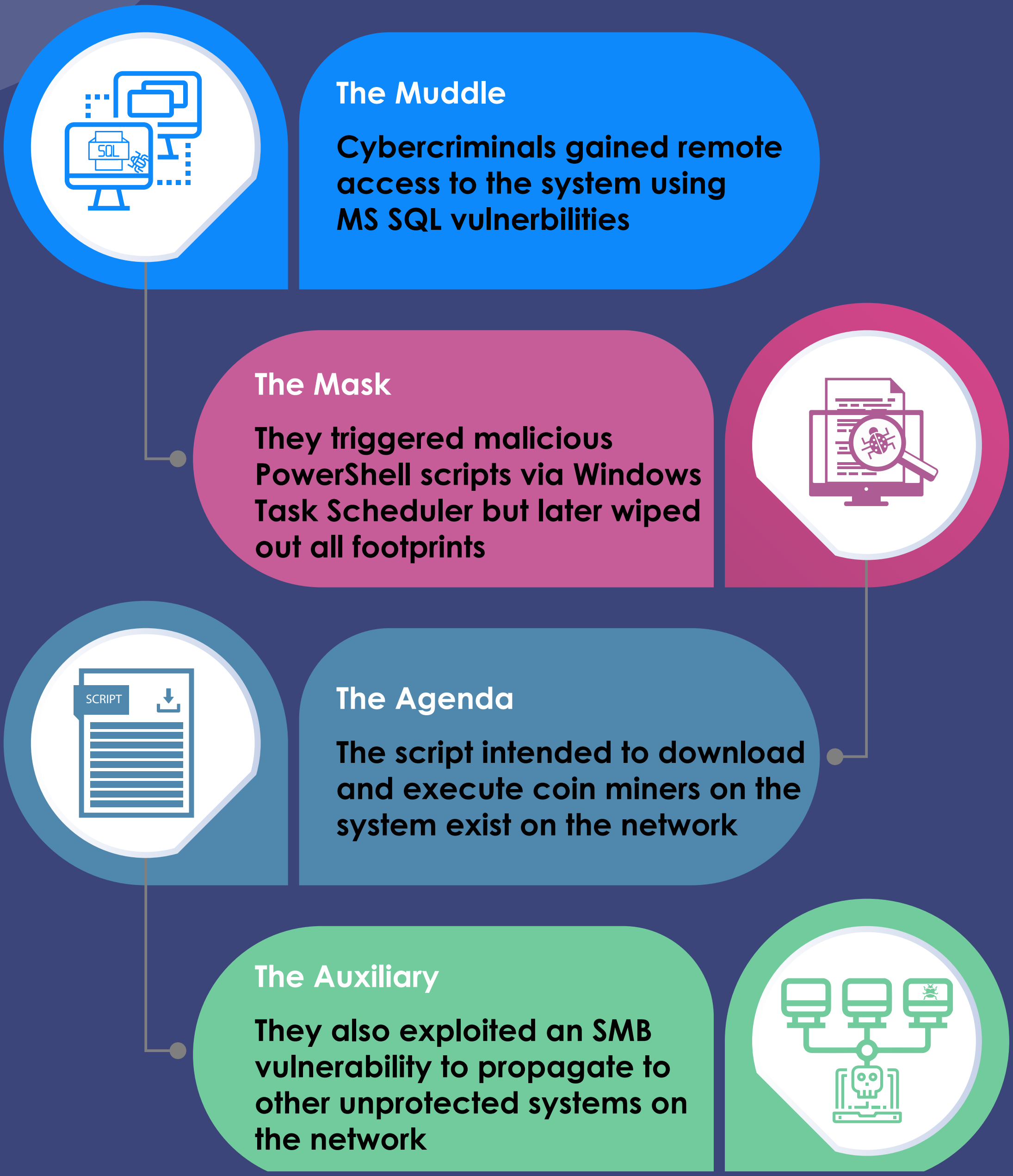
They launched a brute force attack to gain administrator access 3

They executed a .NET-based ransomeware soon after they gained initial access 4

◀◀ Back to contents

Case Study 5 - Threat Actors Exploiting Infamous Vulnerabilities

There was a case of K7 Endpoint Security displaying frequent notifications of a malicious script being blocked on an enterprise network. When the customer approached us to understand why there were repeated alerts, our research team undertook an investigation and recorded the following observations.



The Muddle

Cybercriminals gained remote access to the system using MS SQL vulnerbilities

The Mask

They triggered malicious PowerShell scripts via Windows Task Scheduler but later wiped out all footprints

The Agenda

The script intended to download and execute coin miners on the system exist on the network

The Auxiliary

They also exploited an SMB vulnerability to propagate to other unprotected systems on the network

◀◀ Back to contents

Other Prevalent Methods

While the above-explained instances are a few among the large variety of attacks MSMEs faced during the last financial year, many other attacks are prevalent with high visibility in the threat landscape. The malware strains diversified, and the baddies often picked the best possible fashion of intrusion, such as phishing and other forms of social engineering, among many others.

The other prevalent methods are as depicted:

SOCIAL ENGINEERING
CROSS-SITE SCRIPTING
ZERO-DAY ATTACKS
SQL INJECTION
MALWARE
ADVANCED MALWARE
RANSOMWARE
MALWARE
WEB BASED ATTACK
PHISHING
DEVICE
COMPROMISED/STOLEN DEVICES
DEVICES
BASED
SOCIAL ENGINEERING
DENIAL OF SERVICE
SOCIAL ENGINEERING
ATTACKS
RANSOMWARE
MALWARE
WEB
COMPROMISED/STOLEN
WEB
MALWARE
CROSS-SITE SCRIPTING
PHISHING
DEVICES
SOCIAL ENGINEERING
INSIDER
DEVICE
PHISHING
RANSOMWARE
INSIDER ATTACKS
MALWARE
BASED
ADVANCED MALWARE
SQL INJECTION
RANSOMWARE
DENIAL OF SERVICE
PHISHING
ATTACK
ZERO-DAY ATTACKS
INSIDER ATTACKS
COMPROMISED/STOLEN DEVICES
SCRIPTING
WEB BASED DEVICE
COMPROMISED/STOLEN DEVICES
SQL INJECTION
PHISHING
RANSOMWARE
ZERO-DAY
ATTACKS

◀◀ Back to contents

The Vulnerable Dot

Looking over the threat events that spawned over the year, we found a few security deficits that malicious actors increasingly focus on to get the desired point of intrusion to inflict damage.

These are the most common reasons why businesses fall victim to cyberattacks.

Insider Threats

Most MSMEs operate with a minimum number of employees and have access to enormous business data and systems. Hence, any threat from the inside has a significant potential to harm the business's reputation, data, and finances.

Even though internal attacks sound less severe than traditional malware-based attacks, organizations could lose sensitive information related to research, market strategies, and customer databases due to non-intentional blunders.

Human Error

In modern businesses, many employees have complete access to critical data. Any mistake that happens when they are off-balance, tired, or distracted could result in a security incident. Unfortunately, many recent data breaches or leaks have occurred because of silly mistakes.

Cumbersome BYOD Implementation

Bringing your device (BYOD) brings a series of good impacts, such as working on the go, alongside a few concerns for MSMEs. However, most MSMEs often focus on performance-boosting and ignore the problems, resulting in data breaches. Cybercrime incidents are bound to happen if the employees' devices have access to enterprise data and are not backed up by stringent IT policy.

Shortfall In Employee Training

Every MSME should adhere to a cybersecurity policy that should address good training sessions for the employees via conferences, training, and presentations to shield further attacks on the network. In addition, the training should incorporate basic cyber hygiene, the latest cybercrime trends, and cybersecurity best practices.

Unpatched Systems and Applications

Many businesses often delay updating the software and hardware systems, which inevitably leads to attacks because bad actors look for vulnerabilities in dated systems.

To keep the network safe, install all necessary application software, operating system, and firmware updates on time.

Unencrypted Data

Even though businesses take data backups frequently, leaving them unencrypted poses challenges to securing business data as an unauthorized party could cause a breach by accessing the data contained in the backup. Hence, every business should encrypt all their archived data to ensure its integrity even if it gets breached.

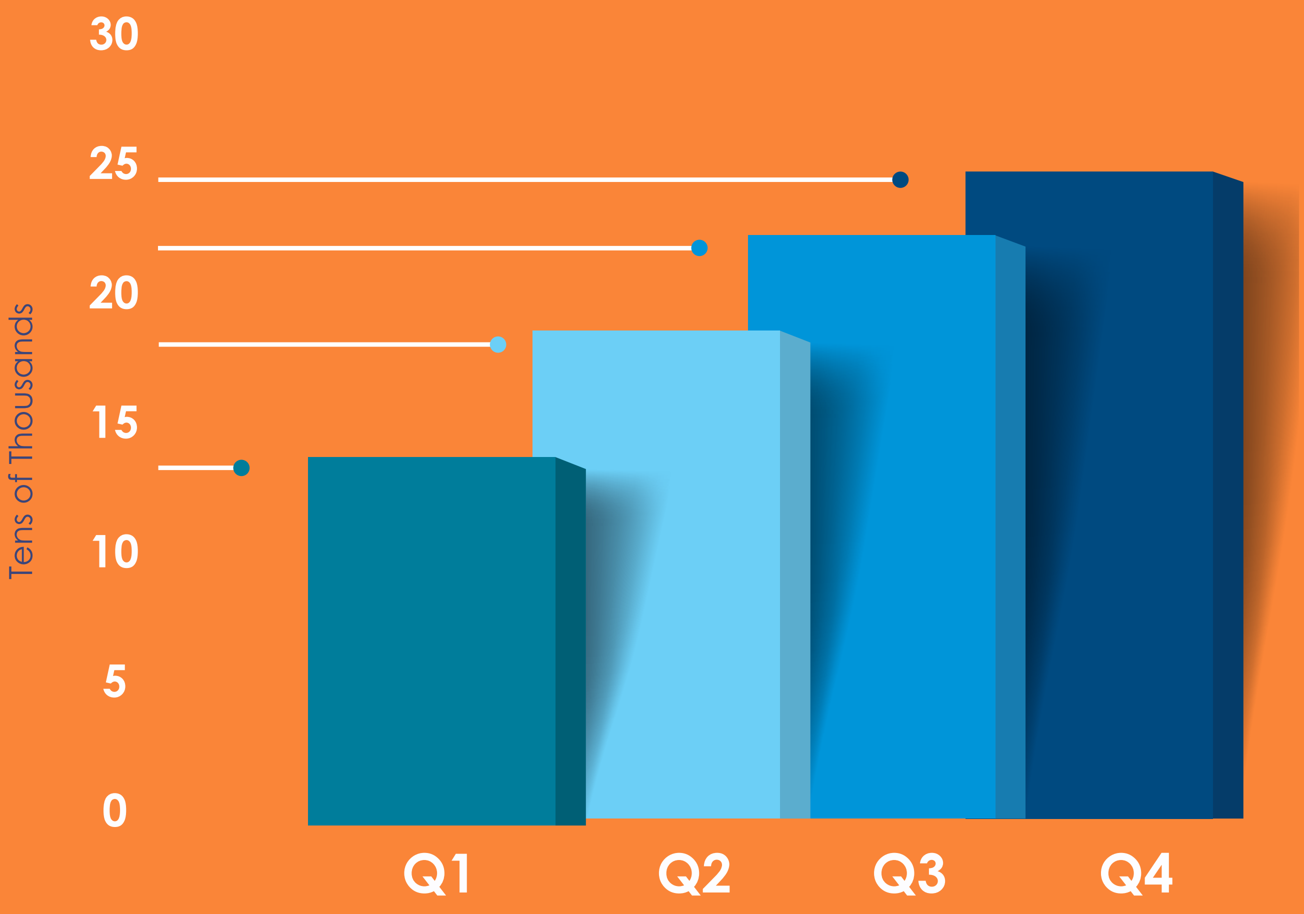
◀◀ Back to contents

How K7 Endpoint Security Helped The MSME Sector

During the financial year 2021–22, K7's security solutions protected over 800,000 endpoints that came under cyber attack. The graph below reveals a dip in attacks observed in the first quarter, but the numbers constantly rose and almost doubled in the last quarter.

This report is, therefore, an attempt to create awareness of the need for cybersecurity for all, with a particular focus on MSMEs, given the enormity and value of this sector, as well as to drive the urgency to ensure the required corrective measures are taken at the earliest, to avoid disastrous scenarios.

Endpoints Protected (FY 2021-22)



Checklist Of Safeguards

K7's range of security solutions provides robust, multi-layered protection against all forms of cyberattacks, including zero-day attacks, drive-by downloads, identity theft, hacked and malicious websites, and phishing, with an extensive set of features that defend against known and unknown ransomware, the nastiest type of malware created thus far.

However, besides having our state-of-the-art cybersecurity solutions installed on networks and machines, you should also incorporate a list of actions, tasks, and rules to outsmart attacks aimed against your enterprise.

To survive the modern cyberthreat landscape, it's always a good idea to nip the problem in the bud by following safety precautions.

Undertake VAPT

Noticing the continuous uproar of website compromise or getting defaced for triggering other menaces such as hosting malware and other nefarious purposes, regular security assessment such as VAPT has become necessary for every MSME out there. VAPT would help identify vulnerabilities and misconfigurations on network assets to ward off breaches, among other pitfalls. Cybersecurity authorities such as K7 Computing offers VAPT services to ensure the security of all parts of the backend infrastructure and web portals.

Backup Your Data

A backup of your data is the primary requirement to prevent missing, corrupted or compromised data.

The best backup-taking medium is external storage devices such as NAS or RAID. Taking backups on the cloud is also a popular option nowadays.

You should always take data backups frequently and once the process is done, you should detach the storage device from the system and keep it somewhere secure.

Never forget to take backups of your cloud archived data on physical storage devices. It can help you immensely if any cloud storage or SaaS service gets compromised.

Encrypt Your Data

Encrypting data is equally crucial as backups. Encrypting data prevents you from leaking any sensitive information to prying eyes.

Patch Everything

We often use multiple devices, operating systems, and application software to meet different business purposes. Each product developer regularly identifies vulnerabilities in their solutions and releases the necessary patches to fix the security holes and improve performance. System administrators should ensure all devices on the network have their OS and installed software updated regularly.

◀◀ Back to contents

Filter Your Email And Train Your Employees

Email is one of the best internet-based tools for businesses of all sizes. It improves communicationbetween people and teams, and with clients. But unfortunately, the growing requirement for email services results in threat actors triggering spam, phishing, and malware campaigns.

Admins should scan incoming emails and quarantine any found malicious. Using a spam filter helps businesses get away from phishing emails. Unfortunately, modern threat actors are smart enough to compose convincing and authentic emails. To eliminate such traps, you must educate your employees on cyber hygiene.

Manage Privileges

Every employee in an industry is responsible for improving their performance and learning new skills. But unfortunately, many aren't aware of the hidden traps on the internet. Hence, you should offer them what they require for work and disable the rest, such as admin privileges on the machine, data modification and deletion rights, etc.

Encourage Password Hygiene And Embrace MFA

Complex passwords protect our online accounts and data from bad actors. But having an easy-to-guess password can get you in trouble. So, always have different and complex passwords for each service.

It would be best if you had Multi-factor Authentication (MFA) wherever possible for better security on your systems. MFA is always better as it involves more than two devices to restrict access.

Most SaaS services offer MFAs, but some stick with 2FA.

Apply Rules To Mobile Devices

We recommend establishing a policy concerning mobile device use. The guidelines should entail restricting app downloads to official app stores only. They should also include necessary cautions, such as going through the user reviews before downloading and installing any app. The guidelines should also provide other dos and don’ts as instructions to employees.

Get Rid Of Third-party And Free Applications

Many MSMEs often have a minuscule budget for the computing infrastructure resulting in security compromises, such as downloading pirated or free software. Some don’t even bother to have security software to evade oncoming attacks. Such negligence can result in massive monetary and reputation loss; hence we recommend securing your devices with reputable security products such as K7 Total Security for Windows, K7 Antivirus for Mac, and K7 Mobile Security (Android and iOS), and keep them up-to-date.

◀◀ Back to contents

www.k7computing.com