Digitaltech Media
Inform, Inspire, Innovate!
▪ Vol I Issue 5 ▪ November 2020

Presented by

Sophos - Ransomware Special Edition

TRENDING STORY

Increased Ransomware Attacks Prompt Organizations to Make 'Zero Trust' their Buzzword!

FEATURE STORY

Educating Clients against Ransomware is the Key, suggest Channel Partners

UAE MARKETSCAPE

Ransomware continues to plague UAE with Key Business Verticals bearing the brunt

Sunil Sharma A Strong Leader of Conviction

Presented by

Sophos - Ransomware Special Edition

SOPHOS

Cybersecurity evolved.

Increased Ransomware Attacks Prompt Organizations to Make 'Zero Trust' their Buzzword!

Ransomware, a malicious software (also referred to as malware), threatens to block access to or publish your organizational data, usually through encryption, unless your company (the victim) chooses to pay the ransom amount/fee to the attackers.

A criminal and money-making strategy, ransomware is installed via deceptive links such as an instant message, website, or email and has the potential of locking computer screens or encrypting files and important data using a password.

But what makes a ransomware attack worse is that in the absence of any payment, your data is gone forever!

That's how severe a ransomware attack can be, and it is precisely why your

> **Sophos offers layered IT security for defending against the latest ransomware. Sophos not only provides best protection at every point, but also provides threat intelligence sharing between all these security points with synchronized security**

SUNIL SHARMA
Managing Director-Sales (India & SAARC), Sophos

SOPHOS
Cybersecurity evolved.

company needs to take adequate measures to safeguard itself against these attacks.

The Ransomware Attack Situation In India

India witnessed several ransomware attacks this year. Some of the most dangerous ones were LockBit ransomware, Magnitude EK (malvertising exploit kit), VHD Ransomware, as well as Wannacry, which is still prevalent in India.

A global survey conducted by Sophos- "The State of Ransomware 2020", published in May 2020 revealed that around 82 percent of Indian organizations surveyed were hit by ransomware in 2019 compared to 67% in 2017.

As a result, data was encrypted in 91% of the attacks that managed to breach Indian organizations successfully.

If one were to determine the average cost of addressing the impact of such an attack in India, including lost orders, business downtime, operational costs, and more, it would amount to nearly ₹80,270,000.

But what is even more alarming is that two out of the three (66%) organizations hit by ransomware in India admitted to paying the ransom.

"Sophos evidence shows that cybercriminals have always used significant regional or global events or holidays as spam lures to help carry out malicious campaigns and scams. We have seen everything from sextortion-like attacks to charitable relief scams," says Sunil Sharma, Managing Director- Sales (India & SAARC), Sophos.

Echoing similar sentiments, Dipesh Kaura, General Manager, Kaspersky (South Asia) shares, "Cybercriminals are always on the look-out for a weak entry point to enter into the network and steal all the sensitive data as well as encrypt it unless the ransom gets paid. This data has also been sold in the underground market, or posted on the dark web by the cybercriminals."

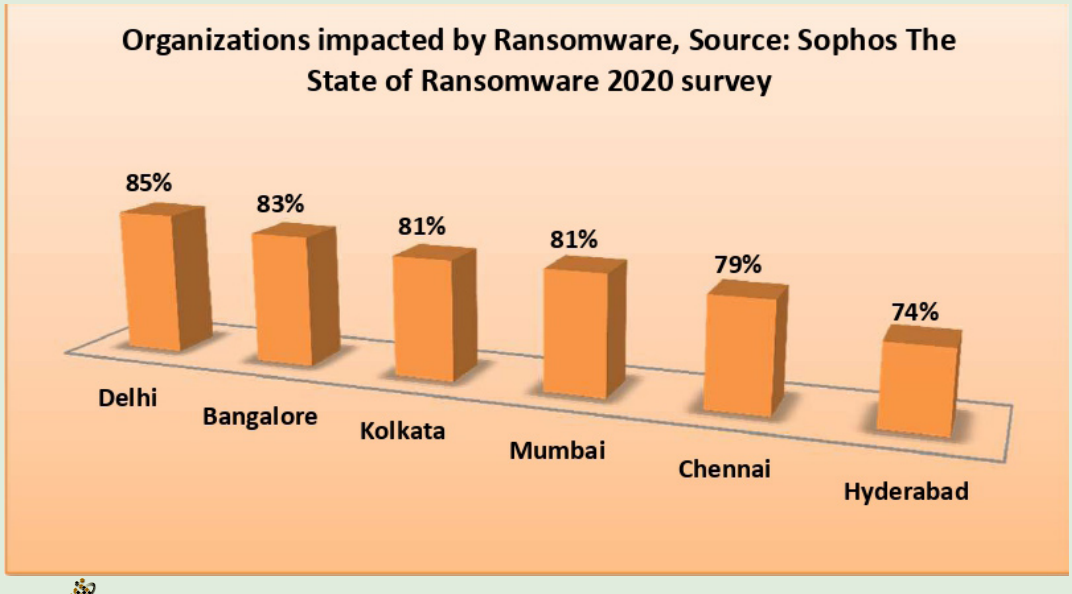
He further elaborates that the work from home culture is an optimum opportunity for cybercriminals to exploit and attack enterprise networks by preying on remotely working employees, using less secured devices.

DIPESH KAURA
General Manager, Kaspersky (South Asia)

> **The concept of ransomware in India first caught attention in 2017 with the infamous Wannacry attack that had impacted India greatly. Since then the attacks have not only increased drastically but have become more targeted, sophisticated and complex in nature**

Also, globally, the scenario is something like this. While India occupies the number two spot among the top 5 countries affected by ransomware in Q3, in terms of the number of attacks, the US tops the list. Sri Lanka, Russia, and Turkey are at #3, #4, and #5 positions respectively.

"It is no secret that



> Organizations should think of preventing attacks before they happen, and not just detect them. A prevention-first strategy is one of the most effective ways to avoid financially devastating data breach

SUNDAR BALASUBRAMANIAN
Managing Director, India and SAARC Region, Check Point Software Technologies

the main incentive of the hackers is money, and sometimes disruption or sabotage. Always struggling to make organizations pay the ransom, hackers find new extortion tactics to leave no escape from answering their demands," points out Sundar Balasubramanian, Managing Director, India and SAARC Region, Check Point Software Technologies.

The Most Impacted Regions and Sectors in 2020

According to Sophos global survey, organizations in Delhi (85%) followed by Bangalore (83%), Kolkata (81%), Mumbai (81%), Chennai (79%), and Hyderabad (74%), were most impacted by ransomware.

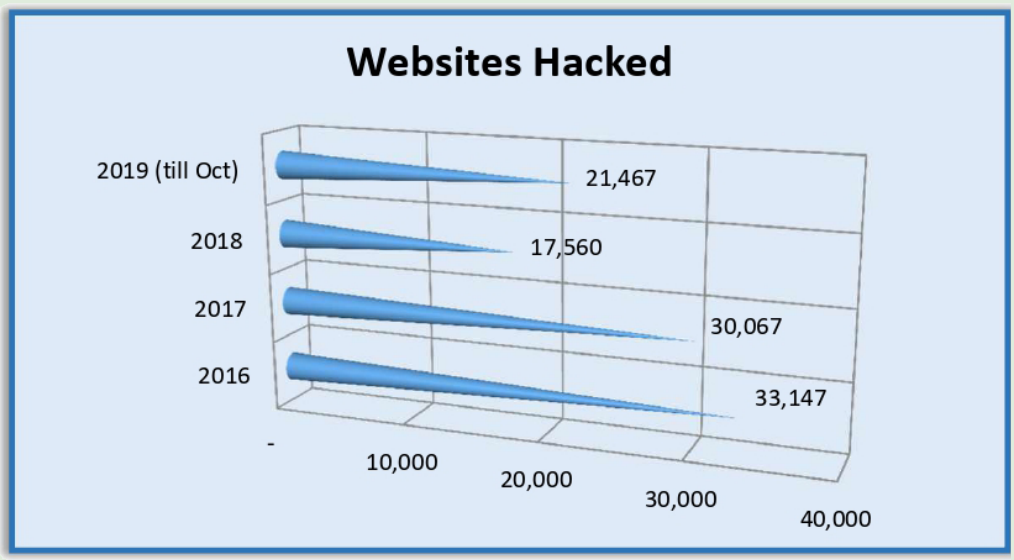
Globally, the most affected sectors of ransomwarehave been the manufacturing industry, followed by the professional services sector which has experienced 17% of ransomware attacks. Government organizations follow in third place at 13% of attacks, as per an IBM report.

"In India, we have seen both enterprises, as well as government sectors coming under attacks. Even media organizations like the PTI and National Highway Authority of India have been some of the big names that have been attacked," states, Rajesh Thadhani, Executive Director – Digital Transformation & Services – Crayon Software Experts India.

RAJESH THADHANI
Executive Director – Digital Transformation & Services – Crayon

> Shift to remote working has contributed to the increase of cyber-attacks. As more devices are connecting remotely and outside the secured corporate network, it is critical to understand how the data is being handled

Indian Websites Hacked (2016-2019), Source: Indian Computer Emerge Response Team (CERT-In)

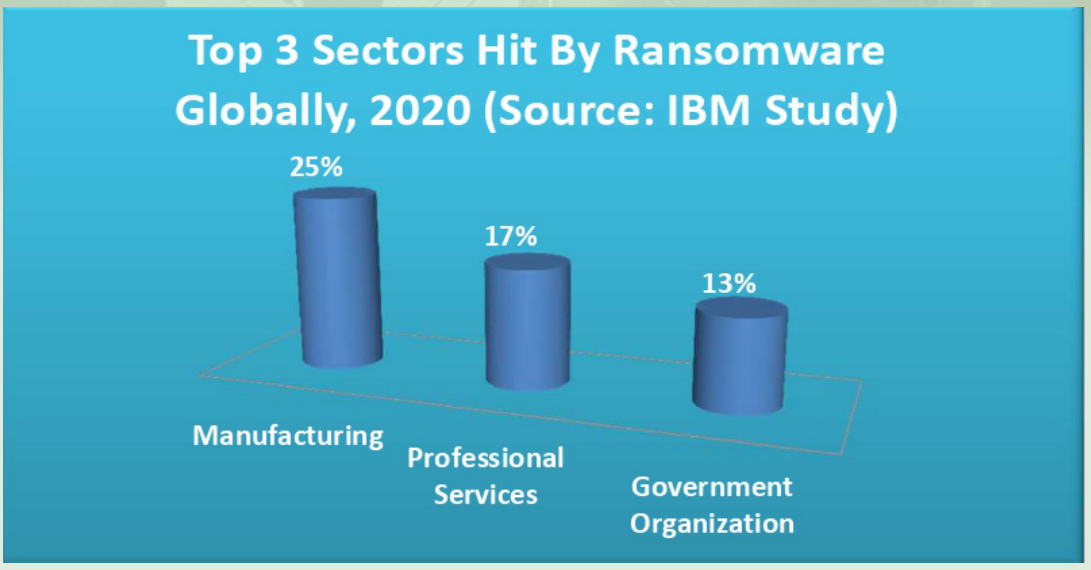


Another development has been witnessed in the form of cyber attackers shifting their aim towards the enterprise market, thus exploiting the lack of cybersecurity awareness amongst start-ups and SMEs.

A Kaspersky research found that of all the encryption families, WannaCry was the most

common. Since the outbreak of WannaCry, cybercriminals have diversified their attack vectors to launch ransomware attacks.

"Cyber attackers are now also targeting SMEs and start-ups owing to a lack of a strong security framework and cybersecurity awareness. SMEs have not paid due attention to their cybersecurity needs, as they were under the impression that they were too small a target for cybercriminals to plan an attack on," states Kaura of Kaspersky.



> **Cybercriminals have escalated their attacks to another level, siphoning off sensitive information from organisations whose files they've encrypted. The belief is that naming and shaming these victims would encourage them to pay the ransom demand**

ADAM PALMER
Chief Cybersecurity Strategist, Tenable

Reasons That Have Contributed to an Increase in Attacks

Lack of specialized cybersecurity teams and constrained cybersecurity budgets make businesses more vulnerable to automated and mass targeted attacks. In addition to this, the need to equip and enable an unexpectedly remote workforce has left companies open to attack.

According to Adam Palmer, Chief Cybersecurity Strategist, Tenable,the shift to remote work has undoubtedly exacerbated ransomware activity as cybercriminals look to infiltrate organizations' networks by exploiting security vulnerabilities in remote-desktop protocols combined with the use of weak passwords.

Many times, it is not just enough to put a cybersecurity layer to the network and devices.

"Cyber-attacks do not just take place in a day. They are meticulously planned and are being put in action to erode the security, allowing the entire network to get hijacked by the attackers. Hence, it is not enough to have a security layer to the networks, and it is more about being constantly aware and mindful of the potential threats," explainsThadhani.

How Can Businesses Best Defend Against Attacks?

Well, according to experts, organizations should adopt the following anti-ransomware measures:

- Train employees how following simple rules can help a company avoid ransomware incidents.
- Always update your operating system and software to eliminate recent vulnerabilities.
- Protect data in the public cloud, private cloud, and on-premises. Almost six in 10 ransomware attacks that successfully encrypted data included data in the public cloud.
- Make regular backups and store them offsite and offline. More than 55% of

organizations whose data was encrypted restored their data using backups in 2019.

- Deploy a layered defense. Ransomware attackers use a wide range of techniques to get around defenses.

As far as Sophos is concerned, the company offers layered IT security for defending against the latest ransomware. Sophos not only provides the best protection at every point but also provides threat intelligence sharing between all these security points with synchronized security through its products such as Sophos XG Firewall, which prevents attacks from getting onto a network. On the other hand, Sophos Intercept X Advanced with EDR detects malicious encryption processes and shuts them down before they can spread across the network.

Similarly, Kaspersky's Anti-Ransomware Tool for Business contains an exploit prevention feature to prevent ransomware and other threats from exploiting vulnerabilities in software and applications.

"Our strategy is to offer a unified security architecture that is supported by real-time threat intelligence," reiterates Balasubramanian of Check Point Software.

Check Point's Anti-Ransomware solution defends organizations against the most sophisticated ransomware attacks and safely recovers encrypted data, ensuring business continuity and productivity.

Conclusion

There is no denying the fact that one in three ransomware attacks are targeted at businesses, and the others aim for banking institutions, government bodies, municipalities, and critical infrastructures.

Thus, organizations need to make 'Zero Trust' their buzzword! Businesses must ensure complete security protection and adopt a prevention first strategy to both detect and prevent ransomware attacks from impacting business continuity.

SOPHOS
Cybersecurity evolved.

SUNIL SHARMA BELIEVES IN BEING THE LEADER WHO EMPOWERS ALL HIS STAKEHOLDERS

The name 'Sunil Sharma' is today synonymous with enterprise channel business in the industry, so much so that there would hardly be anyone associated with the channel community who would not know him. But Sunil has strived to reach that position. In fact his 25 year long career journey in the industry can be best described in two terms - "technology" and "channel sales."

It was during his B.TECH days when Sunil fell in love with technology and he felt himself driven towards it due to its ability to solve problems and empower every aspect of human lives."I was always more inclined towards providing technology and witnessing how it empowers our customers," reiterates Sunil Sharma, Managing Director - Sales (India & SAARC), Sophos.

This inclination, along with his personality drew him towards channel sales. Sincemost companies buying technology rely on channel partners to help make their decisions, Sunil developed an expertise in channel sales andit became a major focus for him throughout his career.

Stint with Sophos

In the cybersecurity industry, the channel has evolved in two ways - Evolution of the role of a channel partner and Evolution of business model. While in the former channel partners now play a bigger role as trusted security advisors in the Managed Service Provider (MSP) space, in the latter they have changed their business model from working with many different vendors to working with a smaller, select group of vendors with which they can grow.

As a channel friendly company, Sophos thinks of its partners' growth right from the product development stage; it therefore has a very strong partner base in India. Sophos creates products with features designed specifically for partners, who on their part have clear upsell and cross-sell opportunities with their existing customers. With his experience of having worked closely with system integrators, value added resellers, distributors, retailers, and OEMs, Sunilfurther boosted the expansion of Sophos' channel base from 300 to 2,500+ partners across India, Bangladesh, Nepal, Sri Lanka, and Maldives.

Talking about his leadership style, Sunil says that it has always been defined to take care of three aspects for the channel -

1) **Mutual growth of Sophos and channel** –"I have always believed in the philosophy of 'Mutual Growth with Our Channel'. We believe in surrounding our strategy and execution around the growth of our channel partners. I believe a channel leader acts like a bridge between vendors and the partner ecosystem. I have always made sure that our partner ecosystem has forward-looking scalable business opportunities that are aligned to our products, services and company vision," he explains.

2) **Role clarity within channel** - Developing role clarity for distributors, partners and the brand's own channel

sales team has always been a core focus of Sunil's leadership. The Sophos Global Partner Program defines roles for distributors and partner tiers. Sophos' channel policy rewards commitment; the more partners are committed to Sophos, the more profitability they can achieve.

3) **Clarity of Communication** - According to Sunil, a clear growth path, partner program and partner enablement tools, all should be clearly communicated to the channel.

When asked about his success mantra, Sunil says that his guiding principle right from the start has been to 'Empower All Stakeholders'. "Customers, channel partners and my own sales and presales teams are three major stakeholders in enterprise channel business. I have always worked to empower each one of them - together they create an equilateral triangle of growth for the technology industry," he cites.

Besides being a Channel Chief, industry folks also know Sunil as a great motivational speaker. To this he says that though on the surface the roles of a motivational speaker and a channel chief look different, but to the core they are same. "As a leader, it is my major Key Result Area (KRA) to keep my team and channel motivated and always looking at the bigger picture to build success," says Sunil while summing up the conversation.

EDUCATING CLIENTS AGAINST RANSOMWARE IS THE KEY, SUGGEST CHANNEL PARTNERS

India stands as the second most targeted country for Ransomware attackers in this pandemic year. This has been highlighted in a survey of 80% plus Indian companies that confirmed that they were hit by Ransomware.

Ransomware has further become a serious concern with the emergence of the 'Work from Home' culture where users are working remotely on a less secured network.

Channel partners or solution providers are well aware of the situation, they now having realized that the number of attacks in recent times have grown five fold.If clients bear the brunt in the wake of any such attacks, service providers too feel equally responsible as the root cause analysis becomes impossible and poses an unalterable damage.

Is Ransomware a Prime Concern?

With over 20 years in the cybersecurity business, V. Anand, Chief Executive Officer,

> Ransomware keeps evolving, getting faster, smarter and costlier. Some ransomware are more complex and harder-to-spot variant than others.

MANASI SAHA
Owner,
Macaws Infotech

Raksha Technologies Pvt. Ltd., believes that ransomware is a big concern for service providers.

"Sometimes, it is irreversible damage, like in a case where data is lost, and there are no credible backups. It becomes an emergency for all involved and casts a big cloud on the abilities of the IT setup, the products used, the service providers involved, everything," he elaborated.

Echoing similar sentiments, Jitesh Chauhan, Director, Rubik Infotech Pvt. Ltd. opined that the threat is increasing every day, thus taking organizations down, and it's only getting worse. As per an estimate ransomware attacks would cost global organizations nearly $20 Billion in 2021.

"The costs associated with any ransomware attack are hard to quantify because you have a variety of direct costs such as the ransom demands (if victims choose to pay them) and remediation costs, as well as indirect costs i.e. downtime, data recovery, lost revenue, improvements to cyber defenses, and reputational damage," he reiterated.

According to Sandeep of ISOEH (Indian School of Ethical Hacking), who is also a CISA certified ethical hacker and Lead Auditor at ISOEH, ransomware is a huge concern for organizations, if not prime. "Ransomware taught businesses that data can be locked without taking it out of the server simply because organizations were neglecting endpoint, which ransomware took advantage of," he explained.

So how are Partners helping to manage the Ransomware Situation?

V. ANAND
Chief Executive Officer, Raksha Technologies Pvt. Ltd.

> We get tremendous support from several vendors. Both our organizations team up well and provide great value to customers. We are provided with licenses, cloud instances, structured training programs etc.

> The weakest and the most neglected assets in any company are the workforce. Most of the companies have never invested in updating their employees on do & don'ts of cyber security

SANDEEP SENGUPTA
Legal Auditor
ISOEH

According to AbhinavVarshney, Asst. Manager Pre-Sales at Satcom Infotech Pvt Ltd, partners need to focus on proactive approach on ransomware infection in the first place, which can be done by educating and testing the end-users through automated

attack simulations, keeping OS and third-party applications up to date and using strong alphanumeric passwords consisting of special characters.

Given that educating businesses is the key, Rubik Infotech has been educating organizations about how important it is to update their Application, Operating System and Password.

Similarly, Macaws Infotech has been providing businesses with best security practices like 2FA, SSL VPN & IPSEC VPN, latest security patches, backup, Server Security, Email Security with EDR, and sandboxing Cloud Security solutions.

> **A Ransomware takes place every 11 seconds globally. Our customers need to be educated of how the growing ransomware threat is evolving and what they can do to minimize risk.**

JITESH CHAUHAN
Director,
Rubik Infotech Pvt. Ltd.

Challenges Galore

Many business professionals seem to cling to a common misconception that the implementation of a malware protection tool provides blanket protection against all potential security risks. Today, critical business IT services are distributed across numerous public and private cloud, web, and server-

hosting environments. Additionally, the mobile revolution, which began a decade ago, introduced more portable endpoint devices, allowing users to access business IT services from any location at any time, and this poses a huge risk before any organization.

> **The solution mixes that we offer are from 'best-of-breed' vendors/OEMs that already have the necessary ecosystem to continually support these throughout the contract life-cycle.**

CAPT. ASHOK B. SHIROOR (RETD.), MD, Mikroz InfoSecurity Pvt. Ltd.

According to ManasiSaha, Owner of Macaws Infotech, the real challenge is about new services. "There are concerns with respect to new service orders, and we are sensing a bit of a slow down," she elaborated. V.Anand of Raksha Technology too feels that budget, quality manpower and process adherence are some of the key challenges in this area.

Capt. Ashok B. Shiroor (Retd.), Managing Director, MikrozInfoSecurityPvt. Ltd., however is of the belief that businesses are unable to adopt suggested measures, as also they are on constrained budgets. "It has become difficult to suggest measures or offer multi-location on-site services for

> Many customers are not willing to adopt cyber security tools as part of the preventive measures. Instead, they are heavily dependent on post cyber-attack services

KAILASH GUPTA
Director, ETSC Computers Pvt. Ltd.

proper solution deployment due to budget constraints," he summarized further.

Vishal Bindra, CEO, and Owner at ACPL, however, feels that the work from home culture is posing a huge challenge. "It gets difficult to ensure that security is implemented and then followed in the right manner," he clarified.

Support from Cybersecurity Vendors

"We are getting good support from Cybersecurity vendors in terms of regular training sessions for our staff around cybersecurity tools and post-attack diagnosis," stated Kailash Gupta, Director, ETSC Computers Pvt. "Vendors are providing free trial and POC tools for us, as well as for our customers, thus making adoption easy. Also, there are various On-demand training tools available from vendors and free credits for Cybersecurity certifications."

Conclusion

Aware of the ransomware situation, partners are starting to offer excellent services to counter the same, thanks to the support they have been receiving from vendors in looking past the challenges and providing apt solutions to their clients. It is only a matter of time before the channel is able to help prevent such situations from arising by working together with the vendor and customer together.

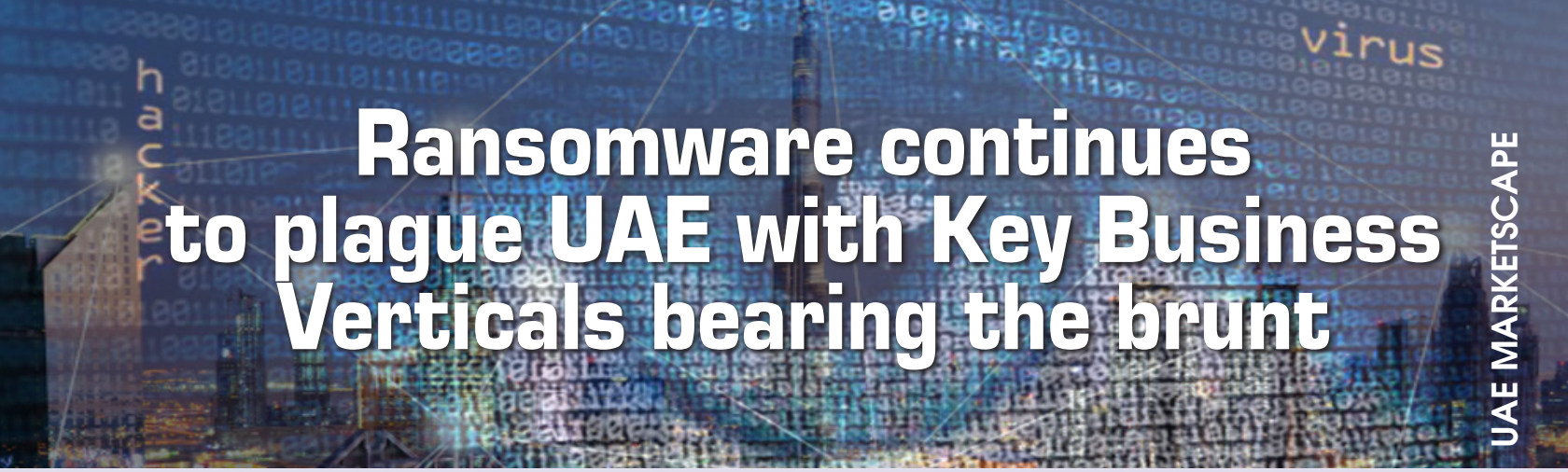
ABHINAV VARSHNEY
Asst. Manager Pre-Sales at Satcom Infotech Pvt Ltd.

> We need to focus on proactive approach on ransomware infection in the first place, which can be done by following security measures like educating and testing the end users through automated attack simulations, keeping OS and third party applications up to date.

> Customers often fail to take proactive steps like Data Security, Data Back-up and recovery process etc. and thus face difficulty in finding apt solution post encryption

VISHAL BINDRA,
Founder & CEO, ACPL

While multiple security vendors claim that they have ransomware protection in their product offerings, it becomes really difficult to protect if organizations fail to follow the best practices of protecting their infrastructure. To make matter worse most of the organizations are hit twice or more by the same ransomware because they don't invest enough in cleansing their systems.



Ransomware continues to plague UAE with Key Business Verticals bearing the brunt

In the wake of the COVID-19 pandemic, UAE has seen a sudden spike in the number of ransomware attacks and therefore it has become a cause of great concern.

Cyber criminals, taking advantage of the pandemic for personal gains have started shifting their focus particularly targeting people working from home and most importantly hospitals. A large number of sensitive data are getting stolen from these hospitals and only on a payment of a good sum of ransom are these attackers coming to terms to release these data. In many case, even after the release of the ransom money, cyber criminals do not part away with the full information taken hostage.

It's important that hospitals have access to their patients' files, more than ever now in the middle of a pandemic. There could be devastating consequences if they are not able to gain access to these patient information on time. An ordinary company could try and get their systems back up and running in a day or two but hospitals don't have that luxury.

But this is a threat that has crippled the nation for long. Last year, a Dubai based contracting firm has been left crippled after being locked out of its own computer systems by a hacker, who then demanded $300 in bitcoins to get the infected machines up and running again. The hacker infected their computers with the dreaded crypto virus, Dharma and left all their files encrypted. Dharma ransomware is one of the most widely spread ransomware infections around the world. The Dharma (. cezar family) decryptor has a complicated decryption process. Unfortunately, there has been no Dharma decryptor released to the public yet from any anti-virus company.

Effects of Ransomware attacks

Ransomware infections result in business disruptions and have an adverse effect on company reputation. It sometimes even becomes difficult to identify the root cause behind the attack. This increasing threat is taking down every organization, whether big or small. These are meticulously planned attacks that are being put in action to erode the security, till it breaks completely and then the entire network is hijacked by the attacker.

On the other hand, a newly released report by a leading security company reveals that ransomware remains a widespread threat in the UAE. For instance, the country accounted for 2.4 million of the 1.7 billion ransomware attacks detected globally in Q1 of 2018. In the pandemic era, the same report states that UAE's ransomware attacks account for 4.27 per cent of the world's ransomware attacks, which is indeed alarming.

Experts have since then warned of a growing spike of such sophisticated attacks not only across GCC but around the globe. The security gaps created by a largely remote workforce have compounded the risk to businesses. In fact, among all the threats in the first half of 2020, ransomware has been a constant threat. Although the number of detected ransomware threats decreased, the survey saw a 36 per cent increase in new ransomware families compared to the same last year.

And thus…

Ransomware, from advanced to entry level is going to dominate the security landscape of 2021. It is therefore becoming increasingly important for organizations to pay attention to ransomware threats and take protective measures. However it is not just enough to have a security layer to the networks, it is more about being constantly aware and mindful of the potential threats.

BEST PRACTICES BY SOPHOS TO BLOCK RANSOMWARE

In a survey conducted by Sophos across 26 countries and with a sample size of 5,000 IT Managers, 51% of the respondents revealed that they were hit by ransomware last year. Attackers in 73% of these incidents succeeded in encrypting data. The average cost to remediate such attacks was a whopping $761,106.

So who are hackers targeting? The answer is – EVERYONE. Another survey conducted indicated that the organization size is not a significant factor for such an attack. 47% of the organizations had fewer than 1,000 employees while 53% had more than 1,000.

Every country, region or vertical market is therefore vulnerable to a ransomware attack.

How can then one stay protected?

A perennial cyberthreat, ransomware will only continue to evolve and it seems just impossible to eradicate them completely. However following certain endpoint protection and firewall best practices can help an organization stay protected from the latest threats. Some of the practices for endpoint protection can be -

I. Turning on all policies and ensuring all features are enabled

II. Reviewing the exclusions regularly

III. Enabling multi-factor authentication (MFA) within the security console

IV. Keeping every endpoint protected and up to date

V. Maintaining IT hygiene

VI. Closing the gap with human intervention

The best practices for firewall would be

I. Including a high-performance next-gen firewall

II. Restricting access to VPN users with the firewall

III. Securing any open ports by applying suitable IPS protection

IV. Enabling TLS inspection

V. Automatically isolating infected systems

VI. Using strong passwords and multi-factor authentication

How can Sophos help?

As a leading security player, Sophos promises the ultimate IT security solution for best protection against the latest ransomware threats. Some of these solutions are –

i. XG Firewall with Sophos Intercept X (endpoint protection)

Having integration capabilities between firewall and endpoint, the protection suite from Sophos offers tremendous advantages in terms of visibility into network health, and the ability to automatically respond to security incidents. Its award-winning XG Firewall, for instance prevents attacks from getting onto the network. Even if a ransomware happens to get on the network, XG Firewall can automatically stop ransomware in its tracks, thanks to its integration with Sophos Intercept X, its industry-leading endpoint protection platform.

Sophos calls this technology Sophos Synchronized Security, that merges its endpoint and network protection features into a powerful, deeply-integrated cybersecurity system. It can be managed easily from the Sophos Central Cloud management console along with all other Sophos products. XG Firewall and Sophos technologies are designed specifically to combat ransomware. XG Firewall's Sandstorm sandboxing and machine learning analysis of files entering the network help ensure that even previously unseen ransomware variants, exploits, and malware don't spread via spam, phishing, or web downloads. Sophos Synchronized Security integrates XG Firewall with its Intercept X endpoint protection to automatically respond to ransomware attacks by detecting the first signs of compromise. Both Sophos Intercept X endpoint protection and XG Firewall together with the CryptoGuardtechnology can detect a ransomware attack in progress, stop it, and roll it back automatically.

ii. Sophos Intercept X Advanced

Sophos Intercept X Advanced with EDR includes all the features to protect the organization from ransomware attacks like Ryuk, Sodinokibi, Maze, and Ragnar Locker. With the help of the anti-ransomware technology, it can detect malicious encryption processes and shutsthem down before they can spread across the network. The Sophos EDR further helps by giving the team the power to ask detailed questions to identify advanced threats, active adversaries, and potential IT vulnerabilities, and then quickly take appropriate steps to stop them.

iii. Sophos Managed Threat Response (MTR)

The Sophos MTR service extends human expertise to the layered security strategy in the form of an elite team of threat hunters that proactively looks for and validates potential threats. If authorized, they take action to disrupt, contain, and neutralize threats, and provide actionable advice to address the root causes of recurring incidents.

Digitaltech Media

Inform, Inspire, Innovate!

WHAT DO WE OFFER?

Digital Marketing

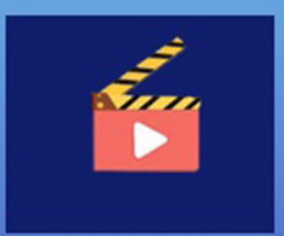
Content Writing

Marketing Collateral

Consulting

Events & Audience Acquisition

Branding



Video & Animation

Designing

Lead Generation

EDM / Banner Design

Visit us - www.digitaltechmedia.in

Contact us for advertisement, video & our services - info@digitaltechmedia.in