RANSOMWARE IS INCREASING THE RISKS AND IMPACT TO ORGANIZATIONS

Cybercriminals constantly engage organizations in a game of leapfrog: system defenses improve, so malware searches for new holes. Recently, ransomware, which has been around since 1989, has been gaining significant momentum. This malware relies on the increasingly simple economics of email attacks (despite the emergence of alternate entry points, email remains a prime attack point), anonymous payment methods, and the growing role of organized groups of criminals.

As a result, cybercriminals collected $209 million in the first three months of 2016 by extorting businesses to unlock their computers. Ransomware is on pace to become more than a $1 billion problem by the end of this year.

Consequently, IT teams need to move quickly to halt this growing attack. First, organizations must educate their employees about the problem and help them to develop good habits that keep corporate information safe.

More importantly, organizations need strong email security services that are able to identify ransomware, prevent it from infecting business computers—or at worst case, help quickly restore data from backups. Armed with those three items, organizations can successfully ward off the growing threat. Without them, they will become tomorrow's news headline.

Shutterstock

WHAT IS RANSOMWARE?

Ransomware is malware that invades a system, encrypts computer files, and blocks legitimate users from accessing their systems. Once installed, the cybercriminals hold the system—and organization—hostage. Unless they are paid a specific sum of money, the system is rendered useless.

Over the past twelve months, ransomware strains have gone from basic to extremely complex and intelligent, resulting in more attacks. What is behind the shift? More organized criminals. The United Nations Office of Drugs and Crime estimates that 80% of cybercrimes are created by organized groups rather than individual criminals. The bad guys view cybercrime as a lower risk, higher reward option than their other nefarious endeavors.

The higher rewards come from the new target victim. The Online Trust Alliance (OTA), a non-profit organization focused on developing online security best practices, found that ransomware attacks shifted from a consumer focus to a business one at the start of 2016. The criminals have invested millions of dollars in contact centers to handle calls from hacked executives and installed ecommerce software enabling victims to more easily pay the ransom demanded for release of their systems. In fact, Infoblox researchers reported a 3,500 percent increase in the criminal use of the net infrastructure that supports ransomware campaigns. As a result, many businesses now find themselves ill prepared to ward off the new sophisticated attacks.

RANSOMWARE ATTACK VECTORS

Ransomware largely targets email transmissions, due to its popularity for business communication and the inherent trust that many employees place in email. And because email is a low cost attack vector that works. A Mimecast report found that 83 percent of businesses view email as one of the most common sources of attack. The damage has been quite significant: More than one-third (37 percent) of respondents experienced email hacks that cost more than $1 million.

An email system can become infected with ransomware in a variety of ways. Phishing is a popular option. Here, the bad guys blanket inboxes with generic messages hoping to snag a few unsuspecting employees. A user clicks on a link or downloads a document, and their system becomes infected.

Spear-phishing is a variation on this theme. Here, a hacker sends an employee an email that looks legitimate—often making it appear to be from an associate, coworker, or a high ranking executive or a department manager. The crook may even send a few messages so the person becomes comfortable with the message's look and feel. After trust is developed, the hacker includes a malicious link or attachment with a message.

Malicious advertising is also gaining traction. Here, workers visit popular sites, say a news source or sports site. The thieves inject malware into the ads on the pages, and unbeknownst to the employee, the ads infect their systems.

Finally, the increased mobility that employees now enjoy has created unforeseen ripple effects. Employees load their USB drives into insecure home computers or local hotspot systems. Malware is downloaded onto the drives. Later, the person opens the file, and the bogus code spreads either throughout their system or worse the enterprise network.

RANSOMWARE CREATES A NUMBER OF PROBLEMS FOR BUSINESSES, STARTING WITH MEASURABLE FINANCIAL LOSSES.

RANSOMWARE'S HEAVY PRICE

Ransomware creates a number of problems for businesses, starting with measurable financial losses. Sometimes, a company feels helpless and pays (usually in non-traceable virtual currency like bitcoins) the third-party to release the files or system.

In addition to hard financial losses, other problems arise. Productivity suffers. Those with an infected system lose access to their data and cannot complete their work. The IT team spends a significant amount of time identifying and remediating the problem at the expense of other projects already on the project list to enhance the corporation's position.

Organizations risk losing valuable intellectual property to the crooks. The OTA found that organized crime groups are targeting businesses with valuable data, putting legal, engineering, defense, and venture capital businesses particularly at risk.

Finally, the brand reputation suffers. Employees, customers, and third parties want to think that the organizations they do business with can be relied upon to keep confidential information secure. Corporations are required by various industry and government statutes to report cyber-attacks, so they must identify any breaches. Once an incident becomes public, the brand's perception drops significantly—as recent high profile break-ins have demonstrated.

RECENT RANSOMWARE ATTACKS

In January 2016, a Lincolnshire County Council (United Kingdom) employee clicked on a ransomware link. The malware spread resulting in the computer systems being shut down for five days and the crooks demanding a £1m ransom.

One month later, Hollywood Presbyterian Hospital was hit with an attack. As the organization troubleshot the problem, the systems responsible for CT scans, lab work, and pharmacy functions were shut down. The email system was turned off, so staff relied on pencil and paper to record patient information. A few patients were referred to nearby hospitals and the emergency room was "sporadically impacted." Eventually, the health care provider paid the hackers $17,000 to unlock its computers.

The Lansing Board of Water and Light, a Michigan municipal utility, was hit with ransomware after an employee opened an email that had a malicious attachment. The malware spread, encrypting files on other computers on the internal network. The organization was forced to shut down its accounting system, email service, and phone lines, including the customer assistance line for account inquiries and the service used to report outages.

How to Prevent Ransomware

Shutterstock

Organizations need to fight ransomware from both a technical and a business process perspective. On the technology side, the organization needs a partner with expertise in the field. In business since 2003, Mimecast's best-of-breed cloud services protect email systems against targeted attacks, data leaks, malware, and spam.

Most attacks feature targeted emails that carry attachments with malicious code. The malware is activated when the employee opens that attachment, leading to ransomware, keylogger, or backdoor attacks.

Begin by reviewing how your email security service can analyze malicious links and attachments in real-time. Ensure macros are not enabled by default across your Microsoft Office application estate, and that 'Protected View' is enabled at all times.

Best practices include either converting email attachments to a safe format or forcing all email attachments to be sandboxed by an appropriately advanced email security gateway. Remember non-sandboxing gateways are not able to recognize or signature macros, as the code is not a viral payload.

You can also disable macros and VBA code in all but essential applications. Blocking USB ports and web-filtering technology can also help against watering-hole attacks.

Review your backup, recovery and archive strategy. Where is your critical data held? What file permissions do users have over network shares? How quickly can you reimage a user's desktop if they ever get infected?

EDUCATION AS A DEFENSE

A technology solution is the first line of defense. Though well intentioned, employees always make mistakes. However, a business also needs to put stronger business processes in place.

First, do not pay the ransom. By their nature, criminals cannot be trusted, so paying the ransom may not guarantee anything other than a questionable item on the corporate expenses sheet.

Businesses need to educate employees about malicious emails. An informed employee is more likely to be more vigilant and spot the telltale signs of ransomware attacks before they take place. Attacks change frequently, so business must stay on top of new trends and conduct internal training regularly.

Employees need to think before they click. Everyone is busy, so when they see familiar branding—including logos and signature lines—workers tend to trust the sender. They should also get in the habit of going directly to the legitimate site through a web browser instead of following an embedded link, especially if it looks suspicious.

Open documents with caution. Employees should view all unexpected attachments with suspicion, especially those with unknown file types. Those individuals working in sensitive departments, such as HR or finance, must be particularly wary.

CONCLUSION

Ransomware is gaining traction in the criminal community. Such attacks are not coming from lone operators working independently. Instead, organized groups of criminals see these attacks as a potential bonanza. Consequently, they have invested a lot of time, money, and manpower in their techniques. Businesses need to keep pace with this sophisticated threat or else they will fall victim to a ransomware attack.