WHITE PAPER

Taking On Ransomware

Market Pulse

The rise of ransomware presents a serious threat to networked enterprises across many industries. Hardly a day goes by without hearing more in the news about this emerging threat and the damage it causes to corporations, individuals, and even law enforcement agencies. But what exactly is ransomware, how big is the threat, and what can enterprises do to protect themselves?

Simply put, ransomware is malicious software that enables cybercriminals to seize an enterprise's computer systems and data, preventing access by employees, customers, and partners until a ransom is paid. Since downtime is extremely costly – and even life-threatening if the target is a hospital or police department – ransomware puts tremendous pressure on enterprises to quickly regain control of their systems and data.

Internet security firm, Kaspersky Lab, provides sobering data on ransomware. In a June 2016 report detailing the spread of ransomware since 2014, Kaspersky Lab reports that the number of users globally who have encountered ransomware "rose by 17.7 percent compared to the previous 12 months (April 2014 to March 2015) – from 1,967,784 to 2,315,931."

In its annual report on internet crime, the Federal Bureau of Investigation reported there were nearly 2,500 ransomware complaints filed last year. "Ransomware has been around for a few years," the FBI said in April, "but during 2015, law enforcement saw an increase in these types of cyberattacks, particularly against organizations because the payoffs are higher."

A new IDG survey of IT managers at enterprises with 500 or more employees also emphasizes the growing threat of ransomware. Nearly 60 percent of responding IT managers said their organizations have been targeted by ransomware, with 55 percent of these respondents reporting that they were unable to block the attacks.

Ransomware costs are considerable

The costs of successful ransomware attacks come in many forms. The IDG survey shows the average cost of a ransomware infection is between $2,000 and $3,000, and these average costs *exclude* any ransom paid to the attackers.

To review the FBI's annual Internet Crime Report, Click here.

The immediate impact of a ransomware attack is on business operations. When employees, customers, and partners are unable to access an enterprise's computer systems and data, business grinds to a halt. Of those respondents to the IDG survey who said their enterprises sustained an attack, 81 percent said the incident reduced employee productivity.

There is also the cost of recovery and remediation following a ransomware attack. IT staff must identify and secure points of vulnerability in the network, thus taking them away from other responsibilities and projects. Enterprises hit by ransomware might also have to pay a

KASPERSKY lab

IDG

disaster recovery services provider. More than half (55 percent) of IDG survey respondents who reported being hit by ransomware cited system recovery as a major cost.

"There's a huge amount of effort that goes into recovering from a ransomware attack," says Andrey Pozhogin, Senior Product Marketing Manager in North America for Kaspersky Lab. "You have to get data back, identify avenues used by the attackers, and determine if your infrastructure is still vulnerable."

If the targeted enterprise is legally required to protect customer data, it could face noncompliance fines and incur legal fees following an attack. Consumer-oriented enterprises would also have to inform customers and might have to purchase credit-monitoring services to protect customers and employees.

Only 21 percent are extremely confident that their employees "know what to do to prevent ransomware from infiltrating the organization."

Finally, the costs can extend to customers whose data was hijacked and partners of the targeted enterprise who may have lost business as a result of a successful attack. This negative fallout compounds the cost to ransomware victims in terms of damage to the brand, customer dissatisfaction, and partner trust and confidence.

How ransomware works

With so much at stake, it is imperative that enterprise IT professionals fully understand the technology behind ransomware attacks and their points of entry into a network. After all, awareness is the first step toward prevention.

The first big wave of ransomware attacks started in 2010 and primarily targeted home users by blocking them from seeing any data on their computers. A message on the target's screen would include instructions to send the perpetrators money in order to unlock the machine.

Blocking, however, is child's play compared to the latest iteration of ransomware: encryption ransomware, also referred to as crypto-ransomware. Whereas technology now allows users to combat blocking ransomware even after a computer has been infected, encryption ransomware requires a special key to decrypt files.

Unfortunately, that key usually resides on the servers of the perpetrators, who will demand a payment – typically in e-currency such as bitcoins – to release the decryption key to the victim. Sometimes the criminals will threaten to have the key destroyed in a certain amount of time if they aren't paid, leaving the victims with no way to retrieve their data.

While ransomware is fairly sophisticated technology, its success in infecting a network often relies on human vulnerability. According to Kaspersky Lab, more than 50 percent of ransomware attacks come from attachments in emails. Using social engineering, a user is tricked into opening an email attachment, which launches the attack.

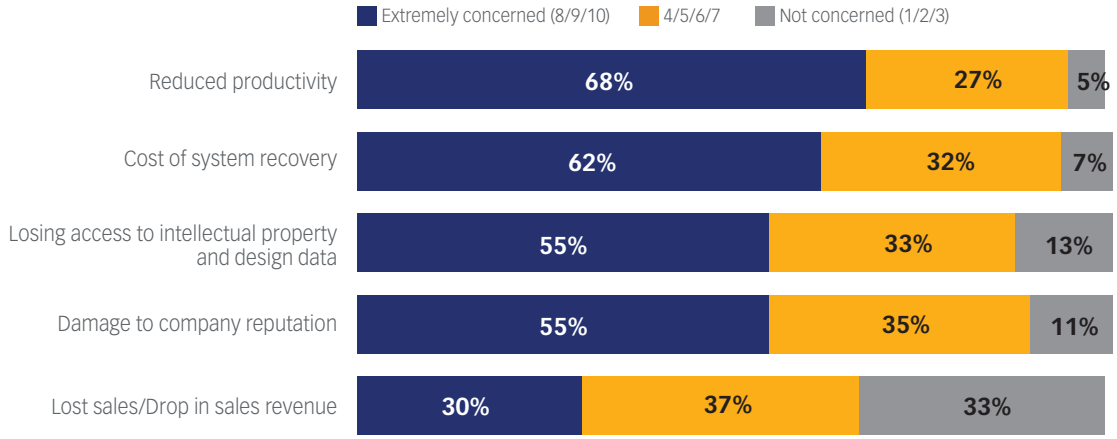
Indeed, many of the IDG survey respondents expressed doubts about the ability of employees to resist future ransomware attacks. Though nearly two-thirds (62 percent) said their organizations have invested resources to educate employees about ransomware, far fewer – only 21 percent – are extremely confident that their employees "know what to do to prevent ransomware from infiltrating the organization."

Ransomware also can attack a network through infected websites and online ads that entice users to inadvertently download ransomware code. But while overly trusting (or simply careless) employees may be the single biggest security weak spot in an enterprise, there also are technological vulnerabilities that allow ransomware criminals to gain control of networks and data. In some cases, rather than identifying specific targets, ransomware criminals use vulnerabilities in popular software like Adobe Flash Player or Microsoft Silverlight to launch the equivalent of random, drive-by attacks.

If successful, these random ransomware attacks are every bit as damaging as ransomware delivered to a pre-selected target. Worse, cybercriminals are persistent and adaptable. Kaspersky Lab reports that ransomware modifications increased 14 percent in the first quarter of 2016 from last year's fourth quarter.

There are an infinite number of ways to drop malware onto a machine, with new methods emerging all the time. Right now, the easiest way to get into an organization is to deceive a user. It only takes one employee to fall for a phishing email to infiltrate a large enterprise.

Level of Concern About Business Impact of Ransomware



SOURCE: IDG RESEARCH SERVICES, JUNE 2016

Ransomware fallout

The impact of successful ransomware attacks on IT systems is twofold:

1) During an attack, IT loses control over the network and the data residing in it.
2) Following an attack, IT must devote time and resources to recovering data, systems, and overall operability.

IT also must conduct forensics to determine how the attack was made, eliminate vulnerabilities in the network, and train (or retrain) employees in security best practices. For enterprises, their time and resources are best spent on prevention of a ransomware attack, including educating employees and implementing a multi-layered security solution.

Of course, the impact of ransomware extends far beyond IT to the business itself. Recent cases highlight the dilemma facing large organizations that have been struck by ransomware. In February 2016, Hollywood Presbyterian Medical Center was hit with a ransomware attack that made medical records inaccessible for more than a week and forced the transfer of some patients to other facilities. While the cybercriminals demanded $3.6 million in bitcoin, the hospital eventually regained access to its data and systems after paying $17,000 in bitcoin.

This is a very common scenario in ransomware situations, Pozhogin explains. "Cybercriminals are very interested in negotiating a reasonable demand," he says. "If the cybercriminals insist on a ransom demand that is too high, this increases the chances the victim will refuse to pay and rebuild their infrastructure from scratch. So they want to show the victim and the world that they can be negotiated with. Otherwise they lower their chances to get money in future attacks."

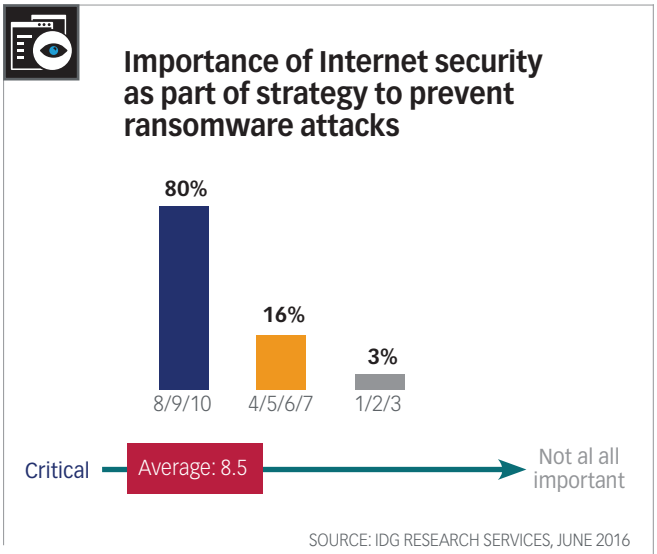
Most ransomware criminals "demand payment in bitcoin," the FBI says, "because it's easy to use, fast, publicly available, decentralized, and provides a sense of heightened security/anonymity."

The FBI does not support paying a ransom to ransomware cybercriminals, and most respondents to the IDG survey agreed. Nearly three-quarters (72 percent) said they were unlikely to pay a ransom, while only 5 percent said their organizations were highly likely to pay.

Those enterprises that do decide to pay the ransom often get an unpleasant surprise: The cybercriminals take the money and run, never providing the victim with a decryption key. A survey of ransomware experts titled "Corporate IT Security Risks 2016" from B2B International shows that 19 percent of businesses did not recover access to their data even after paying the criminals.

IT pros are concerned

Increasingly, ransomware criminals are targeting data-rich organizations such as hospitals, universities, and police departments, which must meet stringent data-protection requirements and thus face tremendous legal or financial pressure to recover their data. In reality, though, any



SOURCE: IDG RESEARCH SERVICES, JUNE 2016

individual or enterprise is potentially susceptible to ransomware schemes.

Given its well-documented rise, it is not surprising that ransomware has grabbed the attention of many IT professionals. Two-thirds of respondents to the IDG survey said they were "extremely concerned" about the threat ransomware poses to their enterprises, while only 5 percent said they were not at all concerned. The average level of concern among all respondents was an "8" on a scale of "10."

The specific concerns of all respondents mirrored the experiences of those who reported being victimized by ransomware. Nearly all respondents (95 percent) said they were concerned about lost productivity, while 93 percent said they were concerned about the cost of system recovery and 87 percent said they feared losing access to intellectual property and data.

Further, one-third of IDG survey respondents said they were extremely confident they can prevent ransomware infiltration, while a vast majority (85 percent) said they have a disaster recovery plan in place to prepare for the after-effects of an attack.

A comprehensive approach

Disaster recovery plans are essential to any enterprise, and they should be thorough and frequently tested. But it is far better and much less costly to deter ransomware attacks in the first place. To effectively combat ransomware, enterprises need a comprehensive, multi-layered security solution that goes beyond simple (though crucial) data backup to include software, services, training, and revamped processes.

The IDG survey shows that the organizations most successful in preventing ransomware infection rely on a variety of technologies, including patch management and mail server security. In addition, the survey reveals that enterprises that have successfully prevented a ransomware attack "are significantly more likely to be investing" in web application security, vulnerability assessment, web server security, and application control. Understandably, then, 80 percent of IDG survey respondents said they consider it highly important to have internet security as a key component of ransomware prevention.

"All those avenues cybercriminals use to infect with ransomware need to be closed to them," Pozhogin says. "We're talking about security for mail servers, web proxy, web gateway. You need proper security on the endpoint."

More than two-thirds (69 percent) of IDG survey respondents said their organizations have budgeted money to deal with ransomware attacks. "It's worth it to invest time, money and other resources to prevent ransomware," Pozhogin says. "If you put together proper prevention tools, you will be way better off than if you are hit with ransomware and recovering."

The B2B International survey shows that nearly half (48 percent) of ransomware victims took several days to recover data, while 29 percent took several weeks or more.

For enterprises uncertain about the return on investment in ransomware prevention, Pozhogin suggests conducting an informal risk assessment test.

"Go to the server room and shut down the server on which your whole enterprise runs," he says. "What happens if the server that holds the data your users are working with goes down, and you know there is no way to restart it in the next seven days? A week of this server being offline with no backup – what is the damage?"

Kaspersky Lab offers enterprises of all sizes multilayered and integrated security solutions designed to protect data and networks from ransomware and other threats.■

Learn more here about Kaspersky Lab products and services.