The Rise of Ransomware

More companies are being held hostage. Spear phishing is fueling the epidemic.
Ransomware is on the rise. Trend Micro reported last month that Ransomware attacks increased 752% in 2016. Gartner analysts estimate that there were between 2 million and 3 million successful ransomware attacks in 2016, and that the frequency will double year over year through 2019.

Even more alarming is the attack vector favored to deliver these types of intrusions is spear phishing. This tactic is hard to defend against traditional cyber defenses because humans unwittingly help the attackers gain a foothold in your network or devices. In fact, 93% of all phishing emails contain encryption ransomware according to a recent report from PhishMe. Ransomware is now synonymous with spear phishing. Your employees are your weakest cybersecurity link.

OLD TRICKS, NEW VICTIMS

This type of attack isn’t new. For years, ransomware extortionists have held millions of consumers’ devices hostage to scam them into buying antivirus software to clean up the mess they created. These small profits were successful and cybercriminals turned their attention to a bigger prize: the business sector. Instead of tens of dollars per attack, they saw an opportunity to make thousands. According to David Goeckeler, senior vice president and general manager of Cisco’s networking and security divisions, no one is safe:

“Ransomware is just everywhere. It’s going after every vertical. It’s one of the most prolific forms of attacking that’s out there. Attackers are making lots of money.”

Ransomware attacks are also becoming more sophisticated, making it harder for the perpetrators to be caught. The use of cryptocurrencies like Bitcoin also make it easier for criminals to reap their rewards without leaving a trace of the crime. This paradigm shift has also been caused by the proliferation of credit card data on the dark web. A credit card number isn’t worth what it used to be
on the black market. Instead of stealing data and looking for a buyer of credit card data to make a quick buck, cybercriminals are turning to ransomware attacks because they create a ready and willing buyer. The victim.

**A BIG PAYDAY**

Ready and willing is an understatement. A study from IBM Security found that 70% of business victims paid the ransom in 2016. Of those who paid, 1 in 5 handed over more than $40,000 to get their data back. And if the cybercriminals choose their target wisely, the payoff can be much larger. Security Week reports:

> “South Korean web hosting company Nayana agreed to pay $1 million in Bitcoin after a ransomware attack hit 153 Linux servers. The attack took place June 10 and resulted in over 3,400 business websites the company hosts being encrypted. According to the Nayana’s initial announcement, the attacker demanded 550 Bitcoins (over $1.6 million) to decrypt the infected files. Following negotiations, they lowered the ransom demand to 397.6 Bitcoins (around $1.01 million).”

**BEYOND THE RANSOM**

Companies often opt to pay the ransom because they fear losing their data or in Nayana’s case, their customers’ data. Quietly paying a ransom also means that the business doesn’t have to go public and suffer irreparable damage to their reputation. According to a Carbon Black consumer study, those consequences are real. Seventy–two percent of consumers are willing to dump their financial institution, 70% their retailer and 68% their healthcare provider if the organization becomes a ransomware victim, the study found.

| Percent of consumers who would consider leaving a business if hit by a ransomware attack: |
|-----------------------------------------------|-------------------------------------------------|
| Their financial institution                   | 72%                                             |
| Their retailer                                | 70%                                             |
| Their healthcare provider                     | 68%                                             |
The costs of a ransomware attack can also extend beyond the actual ransom and reputation damage as SonicWall explains:

“A Michigan utility paid a $25,000 ransom to recover its data, but the attack cost the company $2.4 million in recovery costs, including enhancements to the utility’s cybersecurity staffing and practices.”

Ransomware attacks are a potent threat to organizations because they inflict more than one of the “Five Agonies” of a typically successful cyber attack. They perpetrate every single agony in a single event: direct financial loss, recovery cost, lost productivity, business disruption and reputation damage. Even worse, the risks for cybercriminals are minimal and the payoff can range from hundreds of dollars to millions. A Trend Micro report estimates that ransomware is now a billion-dollar business.

There are a few best practices IT security teams can do to prevent ransomware attacks from wreaking havoc on their organizations. They should ensure that their vulnerability patches are up to date and that data is regularly backed up to get back online faster in case of an attack. But these best practices do not stop the real culprit. Most of the attacks start with a well-timed, malicious spear phishing email. It only takes one email, one erroneous click, for your company to be held hostage.

**PHISHING DELIVERS THE RANSOMWARE**

The easiest way to sneak ransomware past an organization’s security is by infecting a user from the inside. Email makes the perfect vehicle to initiate the attack. Trend Micro reports that 79% of ransomware attacks originate through email in the form of phishing. According to the study by IBM Security, 40% of all spam messages in 2016 contained ransomware. That means that one out of nearly two spam emails is infected. The problem is these emails are becoming increasingly hard to identify as spam or phishing attacks, like that message everyone received from a Nigerian prince asking for their bank account information in return for a small fortune. Verizon noted this change in targeting and attack vectors in their annual data breach report.
“Perhaps the most significant change to ransomware in 2016 was the swing away from infecting individual consumer systems toward targeting vulnerable organizations. Social actions, notably phishing, were found in 21% of incidents, up from just 8% in the 2016 DBIR. These emails are often targeted at specific job functions, such as HR and accounting—whose employees are most likely to open attachments or click on links— or even specific individuals.”

Phishing, spear phishing and social engineering prey on human psychology and its many weaknesses. Emails often look legitimate and use a sense of urgency to get the user to click a malicious attachment or link. An article from Law.com gives the details of one such attack:

“A firm fell prey to a law firm targeting phishing campaign in which attorneys received an email allegedly from the state’s attorney office that alluded to vague legal action against the firm. A PDF baited to contain the details. It also contained ransomware. Like most ransomware, it spelled out a growing ransom over time, and after 48 hours, threatened to delete all encrypted files. When they attempted to restore files from the backups, they discovered that none of the backups worked!”

Cyber criminals use these tactics because they are effective. This success rate coupled with a high probability of a payout through ransomware means that cybercriminals are seeing dollar signs. But there are ways to protect your organization from being phished and then being held hostage by ransomware.

**PREVENT PHISHING, PREVENT RANSOMWARE**

Since ransomware attacks have become synonymous with spear phishing tactics, the best way to prevent ransomware is to prevent phishing. There are a few steps your organization can take to combat these types of attacks: DMARC, Employee Training and Automated TrustGraph® protection.

**DMARC**

Any company with a domain name should consider leveraging DMARC to help reduce spam and prevent phishing attacks. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol specification that protects against direct domain spoofing. It can detect when an email is sent by an unauthorized sender of that domain, and block or discard the message before it is received.

However, DMARC only protects against direct domain spoofing, not all phishing attacks. For instance, it does not detect display name abuse, which is when
an attacker will change the “From” field to look like it comes from a legitimate third party. While DMARC is a good place to start, it only protects against 1 out of 4 types of spear phishing scams. To ensure further protection against phishing attacks, organizations need to also take both a training approach and automated approach to combat these tactics.

For DMARC to protect you against domain spoofing, all of your vendors, partners, and customers (your trusted supply chain) have to implement SPF, DKIM, and DMARC. There is a common misperception that implementing DMARC for your own domain protects you from all domain spoofing attacks that might be targeted at your organization. Sadly, as many have learned, it does not.

**EMPLOYEE AWARENESS TRAINING**

Training your employees to spot malicious emails is another way to lower the probability of a successful phishing attack. However, it will never stop them completely. This year Verizon included the results from its security-awareness training exercises in regard to phishing attacks. Verizon gathered a base of three million users across 2,280 organizations. They then ran 14,000 campaigns. The results were “7.3% of users across multiple data contributors were successfully phished – whether via a link or an opened attachment... about 15% of all unique users who fell victim once, also took the bait a second time.”

These simulated phishing attacks were generic and untargeted. However, the more tailored, spear phishing attacks have a success rate about nine times higher. While the data compiled by Verizon suggests 219,000 people out of three million employees fell for a generic phishing scam, you could expect that number to rise to 1.8 million for spear phishing or social engineering attacks. Regardless of the amount of security-awareness training you provide, your employees are human and they will make mistakes.

**Success rate of spear phishing attacks vs. phishing attacks**

<table>
<thead>
<tr>
<th>Phishing</th>
<th>219,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spear phishing</td>
<td>1.8 Million</td>
</tr>
</tbody>
</table>
THE NEED FOR AUTOMATED PROTECTION FROM GRAPHUS

The data is consistent. Email attacks against humans circumvent your network protections and you only need one employee to take the bait for your company to become victim to a ransomware attack via spear phishing. While the use of employee training techniques and tools like DMARC can provide some protection, they still leave you vulnerable. They do not provide total protection.

Graphus has stepped into this gap in cybersecurity protection. Using graph theory, machine learning and artificial intelligence algorithms to identify trusted relationships between your employees and the people they communicate with, Graphus virtually eliminates the threat of spear phishing and social engineering attacks delivered through email. The solution automatically identifies and eliminates cyber threats. People are easily fooled. Graphus is not.

To identify spear phishing attacks, you must consider DNS, SMTP (email protocol), content and payload analysis, and threat intelligence at the same time. The intersection of graph theory, machine learning, and artificial intelligence led to the development of a TrustGraph® that can be built programmatically for each organization in real time. Patterns of interaction between people, devices, and networks provide insight into what communications can be trusted and which exhibit suspicious behavior.

The learnings were packaged into a simple, powerful, automated system that anyone can use because it works automatically on your behalf. Employees are protected from malicious emails before scammers can fool them with manipulation techniques based on human psychology. Graphus provides a dashboard that shows exactly what is going on, where you are being attacked and how to investigate further. However, most users rarely need to consult the dashboard because Graphus protects them automatically.
YES, YOU CAN PREVENT RANSOMWARE ATTACKS

Organizations don’t think it will happen to them until they are held hostage. Ransomware attacks can cause irreparable damage to your organization’s bottom line, reputation and business operations. The best way to protect yourself from ransomware attacks today is to prevent yourself from becoming the victim of a spear phishing attack. Graphus protects against spear phishing emails which prevents over 90% of all ransomware attacks from ever reaching your IT assets. You can lock down your networks, but you can’t lock down the ability to communicate with the outside world. Don’t leave it up to chance. Protect yourself today with Graphus.

REQUEST A DEMO