Top 4 Threats 2016

December 27, 2016

**Lore Systems Inc.
Lore.net**

**For more information, contact
twong@lore.net**

In 2016, security teams were attacked by over 90 million cyberattacks. Some experts are predicting number could double in 2017[1] with staggering economic impacts; it's estimated that the likely annual cost to the global economy from cybercrime is more than $400 billion which is more than the national income of most countries.[2]

And while high-profile attacks make the news, most organizations need to know where to focus their everyday cyber security efforts. According to the IBM X-Force Threat Intelligence Quarterly, 4Q 2015 report[3], inside threats, ransomware, multi-layered and morphing "onion-layer" attacks and increased boardroom scrutiny are among the four emerging trends that every security team needs to look for.

Trend 1: Multi-level or "Onion-Layered" Security Threats

Onion-layered security incidents involve multiple coordinated or independent simultaneous attacks on the network. The first layer is a rookie type of hack, generally loud and easily detectable; the second layer of intrusion is generally more sophisticated, difficult to detect and more damaging. Independent layered attacks are usually found accidentally. While diagnosing the top-layer amateur hack, the cybersec team discovers an unrelated but more sinister hack that was hiding in the system.

In a coordinated attack, the initial layer of intrusion intentionally masks a second more damaging attack. An example of this type of "onion-layered" attack is a first line distributed denial of service (DDoS) attack, leaving just enough bandwidth for a the second more sophisticated and sinister hacker to sneak in and exfiltrate data while the security team is preoccupied with restoring service.[4] Because the security team focused on the DDoS attack, the sophisticated hack can go undetected for weeks or months while the "layers" are peeled back and the root cause is found.

IBM states that "Of all the incidents that the [IBM Emergency Response Services] ERS teams encountered, these complex, multi-layered attacks were the most demanding of investigative time and resources to ascertain the facts, find the root causes, develop a timeline of events, and provide the client with recommendations on how to resolve the issues that allowed the attackers to get into their network."

How to Mitigate Layered Security Threats:

◦ ***Keep systems updated.*** Many first layer break-ins are due to internet-facing servers running old unpatched, unsupported operating systems.

◦ ***Don't ignore security alerts***. Most organizations run anti-virus software and use anti-intrusion firewalls. However, they often don't bother reading the logs or following up on the alerts the systems give them. Instead these organizations respond only to major service interruptions, allowing vulnerabilities to exist long after they were announced. This is even more tragic considering the number of affordable, accessible tools in existence that break down your logs into readily actionable reports.

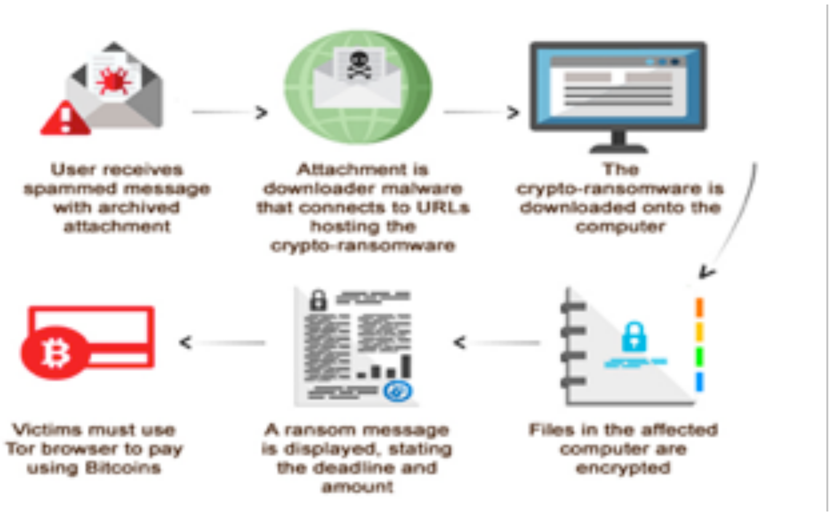
◦ ***Listen to what your network is really telling you.*** When a server acts up it is easy to focus on finding and fixing the primary issue. However, it is only after peeling back the layers of an attack, that the root cause of an issue is found. Finding and removing malware should be an alert that a security breach has occurred; repeated or multiple user lockouts should prompt questions as to whether password databases have been compromised. By looking past the first layer of issues you are likely to uncover deeper issues.

◦ ***Periodically test vulnerabilities.*** Performing penetration testing exercises will help with early identification of those systems and applications that have vulnerabilities.

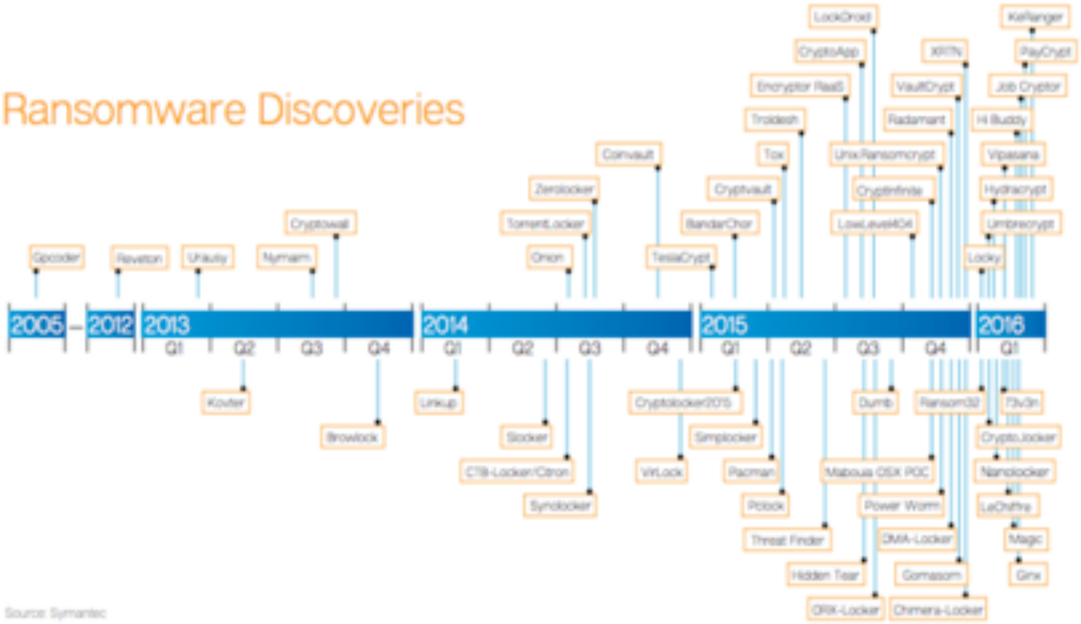
Trend 2: Ransomware

As the name suggests, ransomware is a type of malware that steals something from a user and demands a ransom to get it back. Generally ransomware falls into one of two categories; the first category of ransomware locks a user's system and tricks them into thinking they have to pay a ransom to unlock it. This type of ransomware is more innocuous, because no actual damage is done to the infected system and no information is actually lost.

The second category of ransomware encrypts all system data, making it inaccessible and unusable. Ransom instructions are generally left as text files and a company is unable to access or decrypt the data until it pays the ransom amount. Some of the most well-known ransomware attacks go by the names CryptoLocker, Locky, CrytoWall, or Winlocker.


User receives spammed message with archived attachment
Attachment is downloader malware that connects to URLs hosting the crypto-ransomware
The crypto-ransomware is downloaded onto the computer
Files in the affected computer are encrypted
A ransom message is displayed, stating the deadline and amount
Victims must use Tor browser to pay using Bitcoins

Ransomware costs are more than just pocket change; Hollywood Presbyterian Medical Center had to pay $17,000 to hackers. MedStar Health in Columbia, Maryland had to pay $19,000 to have their data decrypted. Needless to say, ransomware is a growth industry, with attacks increasing 300% last year according to the FBI[i] This dramatic increase is confirmed by Kevin Haley, the director of product management at Symantec Security Response, who recently reported that his group has seen an average of over 4,000 ransomware attacks per day since Jan. 1. This data shows a 300-percent increase over the approximately 1,000 attacks per day in 2015.



Ransomware Discoveries

Source: Symantec

The FBI has become more involved in Ransomware attacks and discourages payment of ransom. The agency has noted in its 2016 report that the overall average cost of remediating a successful insider attack is around $445,000. With an average risk of 3.8 insider attacks per year, the total remediation cost of insider attacks can quickly run into the millions of dollars.[ii]

How to Mitigate the Threat of Ransomware:

- ***Backup, backup, backup:*** A complete, reliable backup plan is the only way to prevent ransomware. Restore points are ineffective. The only way to recover a computer's data without turning to hackers is to have a backup to restore a computer to its pre-attack functioning.

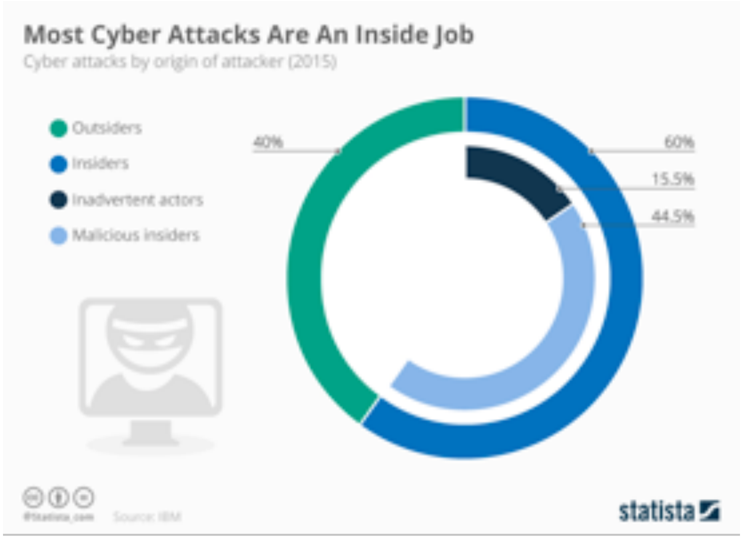
- ***Keep systems updated***. Many first layer break-ins are due to internet-facing servers running old unpatched, unsupported operating systems. When security updates aren't applied promptly, ransomware can exploit these systems to give attackers access to the system resources they want to lock or the data they want to encrypt.

- ***Practice the basics of prevention***: Many ransomware attacks can be prevented with basic but essential network security. These steps include mapping all network drives to authorized users to keep unauthorized users (hackers) from accessing the PC and making folders unable to be altered (read-only) to keep hackers from putting files into the PC that will encrypt data.

- ***Teach safe computing practices***: Teach users when it's "not ok" to click on a link and how to recognize and report the signs of phishing attempts is one of the most effective first-line defenses in keeping ransomware off your server in the first place.

Trend 3 - Insider Threats

More than half of all malicious cyber attacks are inside jobs, and some experts suggest that as many as 80% of all security breaches are caused by a company's own staff. According to a 2015 Price Waterhouse Coopers[iii] report employees were the biggest cause of security incidents surpassing hackers, contractors, and organized crime.



This Statista chart utilizing the data from the IBM X-force report, shows how important it is to teach employees safe computing practices.

An insider attack happens when a poorly vetted contractor or disgruntled employee prepares for a future attack by installing a remote administration tool (RAT) like TeamViewer for future access to the employer's network. Other common access methods involve exploiting organization's lax security policies to access valid network pathways, shared VPN accounts and easily guessed logins to tunnel back into the employer's servers, even if the employee has been terminated and his user account disabled.

According to the X- Force Report, these easy exploits "give insiders with ill-will toward their an organization powerful weapons to express their resentment.", According to a recent survey by

Crowd Research Partners, the overall average cost of remediating a successful insider attack is around $445,000. With an average risk of 3.8 insider attacks per year, the total remediation cost of insider attacks can quickly run into the millions of dollars.

How to Mitigate Insider Threats:

- ***Know your employees.*** Be diligent in background checking employees, particularly IT staff - who may have greater access to sensitive data than anyone else in the company. Equally as important, be very careful with outsourcing contracts; unless the terms and conditions are carefully-worded, you may find you have little control over the quality of staff hired by outsourcing partners.

- ***Use and enforce strong password policies.*** Don't allow shared user accounts or administrator passwords. Many passwords may be written on sticky notes under a keyboard for "easy access." Another important policy is to require secure passwords, (not a user's favorite football team) and set them to automatically expire. These simple policies, when enforced, make it much easier to lock out a fired employee or disgruntled contractor.

- ***Periodically screen the network for RATs.*** Monitor outbound traffic, and screen for commonly known RAT tools. If any are found one solution is to use a domain name server to block access for the master server. This can be difficult because RATs often change, add and remove master servers on a routine basis.

Trend 4 – Increased CEO awareness

In 2015, cybersecurity became a true concern at the boardroom level with more positions of power asking questions about their organizations' security posture. CEOs are recognizing that proper cyber security requires integration of cyber risk management into day-to-day operations. In fact, a recent survey of CISOs by SMU and IBM, revealed that 85% of CISOs said upper-level management support has been increasing, and 88% said their security budgets have increased, noting that news coverage of large and harmful security breaches was the driver of that support.[iv] Given this higher level of awareness, it is essential that security teams keep top level executives informed, educated and assured that the organization is prepared to respond to a breach, restore normal operations and ensure that assets and the organization's reputation are protected.

How to Instill Confidence in Your Organization's Preparedness:

- ***Tabletop exercises.*** Post-incident critiques often confirm that experience gained during emergency response exercises was the best way to prepare teams to respond effectively to an emergency. Exercises should be designed to engage team members and get them working together to manage the response to a hypothetical incident.

Exercises enhance knowledge of plans, allow members to improve their own performance and identify opportunities to improve capabilities to respond to real events.[v]

- ***Emergency Response Plans.*** According to the IBM X-force report, organizations have begun anticipating security incidents and planning for them. Recently, the Federal Communications Commission created the Small Biz Cyber Planner to help businesses evaluate their current cybersecurity posture and create a plan[vi]. The plan should focus on key areas including:

  1. Prevention: Solutions, policies and procedures need to be put in place to reduce the risk of attacks.
  2. Resolution: In the event of a computer security breach, plans and procedures need to be in place to determine the resources that will be used to remedy a threat.

  3. Restitution: Companies need to be prepared to address the repercussions of a security threat with their employees and customers to ensure that any loss of trust or business is minimal and short-lived.

  Having advance plans for breaches create the ability to respond quickly and efficiently. This type of response "may mean the difference between a short-duration event with limited impact and a long running disaster." Written response plans also lend themselves to a boardroom environment, where reports are the primary medium of communication.

- ***Risk evaluations:*** Given the high cost of security incidents many CEOs are more willing to spring for the high cost of a full threat assessment. In order to maintain an accurate, big picture understanding an organization's security preparedness, CEOs necessarily solicit and distill security-related concerns. Risk evaluations help CEO's think of security breaches in terms of "when" not "if" and security teams should welcome the opportunity to find, and shore up defenses

Conclusion

The key takeaway is that there are any number of tools and software offerings out there that will mitigate, protect and report. However, the first and most important line of defense is a thoroughly written and fastidiously executed security plan that includes all departments; HR, Operations, C-level, IT; security practices do not stop with security professionals. Organizations that sow and foster a deeply rooted culture of security and accountability will be able to withstand the persistent, dynamic nature of cyber threats.

For help creating a comprehensive plan for your organization, contact Lore Systems. Each of our experts has a minimum of ten years hands on experience in identifying and implementing tailored IT solutions for any business.

[i] http://www.riskmanagementmonitor.com/wp-content/uploads/2016/09/Ransomware1.jpg

[ii] http://www.darkreading.com/vulnerabilities---threats/survey-shows-insider-threats-on-the-rise-organizations-experience-an-average-of-38-attacks-per-year/d/d-id/1321069

[iii] http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

[iv] https://www.smu.edu/News/2015/smu-deason-cybersecurity-risk-study-27oct2015

[v] https://www.ready.gov/business/testing/exercises

[vi] http://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide_1.pdf

http://www-03.ibm.com/security/data-breach/cyber-security-index.html