Ransomware: Not Your Typical Threat

Lower Ransomware Risk with Education, Planning, and Relationship Building

by Jon Leer, Writer, Leer Technical Communications, LLC

Interviewed: John Galda, Director of Risk/Security at Charles River Development

© Valerijs Novickis

While security solutions continue to sprout up all over the globe promising firewalls of protection against barbarians at the gate, ransomware attacks increase against small and critical businesses. Rather than going for the big trophy enterprise, ransomware hackers use unsophisticated, easy to build malware to harvest the easy cash from their victims. Before the attack, the potential threat goes undetected by IT – there is no known signature. After the attack, local, state, and federal authorities have difficulty tracking the culprits.

What's So Unique about Ransomware?

What is it about ransomware that is making malware vendors scramble, small businesses cringe, and authorities close cases as "unresolved"?

Ransomware is an elusive threat from unknown and often unsophisticated entities. Its key attributes are:

- Attacks small businesses often with critical services (e.g., healthcare)
- Hard-to-detect because it has no known signature and is easily modified

- Blackmails the victim by shutting down data access and promises a significant loss of business
- Demands a cash ransom to restore data access and prevent loss of data
- Leaves negligible fingerprints for identifying a signature with threat code left behind for analysis
- Remains under the radar of local, state, and federal authorities

John Galda, Director of Risk/Security at Charles River Development, notes that larger companies typically make large investments in sophisticated security solutions. When such a company is attacked, it is by a hacker who is a code expert and deploys a sophisticated malware package with severe intent, such as data theft (e.g., privacy and financial data) or chaos (DDoS).

Small companies typically do not have the resources to invest in such comprehensive security solutions. These companies are the “low hanging fruit”. They are unprotected by limited IT resources, ignorant about cybersecurity best practices, and unable to detect and remediate threats unknown to their Anti-Virus software – a perfect recipient for ransomware.

© Clifford

> *“[consider] the planes of the Serengeti. The lion takes down a water buffalo and will eat well. If the lion were to turn to eating mice it would starve… We’re not seeing the lions in ransomware. It’s a lot of jackals and dogs who are going after the easy targets, buying other people’s crimeware… Going after the low-hanging targets.”*
> **John Galda**

Galda suggests that ransomware will continue to grow and elude the experts, focusing on smaller businesses and vulnerable enterprises (e.g., healthcare) where security controls may not be as diligently deployed and monitored, and employee security hygiene less than pristine.

Pain Points

Consider the difficulty of dealing with ransomware.

Limitations of Signature-Based Detection

John Galda adds, “The problem with current malware solutions is that they are signature-based.” Only when somebody is attacked and the malware code retrieved and analyzed does the signature become known and is finally added by security vendors to their updates.

Ransomware attackers are betting on being able to “harvest” the ransom before the ransomware count-down timer hits no time left (i.e., pay up or lose all your data).

Should I Pay the Ransom?

Apparently, many companies would rather pay the ransom than go through the lengthy data analysis and recovery. Another sore point is that the authorities and courts will probably never catch the bad guys. The malware might be retrievable, but identifying a signature may be fruitless since the malware can so easily be modified.

The common victim mindset during an attack is that “I need it now” and “I don’t want to pay the attacker.” But the time is running out before all data will be lost. And restoring the infected system is going to take a while. In the end, without any immediate response plan in place, the company may need to pay the attacker.

There are ways to reduce the risk of a successful ransomware attack. These include educating your employees, assessing your data assets associated risk, creating and practicing a recovery plan, and building better understanding with other management about common security risks and strategy.

Educate and Share Best Practices

At the SC Congress Boston, John Galda sat on the Ransomware panel, which noted the importance of in educating employees, partners, and customers about good security practices in non-technical terms to help mitigate not only threats from outside but also from within. Top suggestions include:

- Schedule on-going backups of critical data
- Share good security hygiene
- Set up strict change control and access
- Schedule application scanning
- Purchase cyber insurance
- Perform risk assessments

- Train employees throughout the year (relationship building)
- Build better relationships within the C-suite (CIO/CSO) and board
- Build in redundancy
- Monitor programs and procedures for a culture of security
- Plan for the worst, and ensure there is a rational response plan in place and TEST IT – consider different scenarios
- Be careful what you say about your security to others
- Run desktop exercises to test dealing with an attack
- Test restoring data from backups
- Layer your security on email. John Galda adds, “Office 365 has a layer of security, but it may not be enough. You may need to add something stronger, such as adding a Baracuda solution.”

John Galda comments that ransomware is typically a reactive experience, so you want to be prepared. Essentially, you do not want to “have a flat tire, and discover that there is no tire in the trunk.” Because ransomware is “opportunistic” (you will not know what part of your data infrastructure is affected), you should create a heat map of where critical data is located and identify what needs to get backed up regularly. If an attack occurs, you know the critical data is already backed up no matter what data is affected by the ransomware.

Commit to Building Better Relationships

Ensuring a successful outcome following a ransomware attack depends on the commitment to being proactive. The key stakeholders are the employees, IT, and management. Management must be on the same page to devise a practical plan that can be implemented by the entire team.

CSOs and CISOs are recognizing that they need to bring the other executives in the C-suite into the security fold. This requires relationship-building skills. CSOs are usually looking over the horizon, and should be performing risk assessments on an annual basis. However, they also need to work in conjunction with the CISOs to strengthen their credibility with CFOs and CEOs so that they can share in the ownership of risk assessment and planning.

The bottom line is that the more educated the entire team is about cybersecurity, threats, and possible intrusions, the lower the risk of a successful attack.

Think Ahead of the Curve: Evil is as Evil Does

To go beyond relying on only known malware signatures, we need to think differently. John Galda notes that the new paradigm is to consider behavior-based activity which detects evil is as evil does. For example, you download something to your machine, and it is not recognized as the signature from known malware vendors and it starts “doing stuff”, such as doing an unpack and writing something to memory, port scanning, or making a copy. Ideally, the behavior analysis software would detect “you aren’t supposed to do that”, and move the activity to a sandbox for further testing before allowing it into production.

However, looking at behavior is difficult, because what is evil? Unfortunately, log analytics alone cannot define and detect evil. We should look at both user and machine behavior for answers. Many malware vendors are now on this quest. For example, MalwareBytes Labs advanced threat research arm researches and investigates telemetry data from millions of installations, and offers an advanced behavior-based detection engine. John Galda predicts that approach will be a good end game for threat detection and remediation, but getting there will probably be painful

In Conclusion

We may not have a 100% failsafe solution for ransomware attacks, but you can greatly reduce the risk by educating your employees on security hygiene, religiously following best practices such as backing up and testing restores, and building better relationships amongst members of the C-suite for improved security and risk assessment and disaster recovery planning and execution. To extend automated solutions to further, we must embrace new technology that shortens the time to recognize bad behavior as threats, and isolate those components for successful remediation.

About The Author

Jonathan Leer, Director of Communication, of Leer Technical Communications, LLC. For the past 25+ years he has been providing technical and business writing services to small-to-large businesses. Several are in the security industry, including RSA and Bradford Networks. He has published articles for Entrepreneur, Workforce Management, Sales Management, and Training. Jon can be reached online at jleer@leertech.net and at http://www.leertech.net.

About the Subject Matter Expert

John Galda, Director of Risk/Security at Charles River Development. He is an expert in Risk Management, IT Governance, and Security Awareness, John has 30+ years of experience in information technology at Fortune 500 companies such as General Electric, Liberty Mutual, United Technologies, and Textron. John is a Certified Information Systems Security Professional (CISSP) from ISC2, Certified Information Security Manager (CISM) from ISACA and is also certified in ITL, LEAN Six Sigma and Project Management from George Washington University. He has a Bachelor's of Science in IT, done graduate work at Harvard, and has two Master degrees, the most recent an MBA from Boston University.