Words: 1627

Behavior Analytics – Moving Beyond Signature-Based Malware Solutions

Ransomware: Educate your people, and look to new technology

By: Jon Leer

Phone: 603-315-4029

Email: jleer@leertech.net

Publication: CEOWORLD

With recent cybersecurity attacks occurring around the globe, despite the abundance of available security solutions and education programs, ransomware continues to thread its way through the gauntlet of layered security devices and applications, continuing to force victims into submission – the reward is easy cash for little work. This article describes how security solutions providers, large and small, must rethink their approach to providing effective cybersecurity solutions.

Executive Summary

With all of the available security solutions, ransomware continues to thread its way through the gauntlet of layered security devices and applications, continuing to force victims into submission – the reward is easy cash for little work. Although primarily affecting SMB (Small Medium Business) prey, it is only a matter of time before malware barbarians will be at the larger enterprise gates, as well as cloud resources.

Signature-based solutions no longer work. And purveyors of Ransomware are getting bolder with the possibility of stretching outside the SMB zone of easy money to pursuing large enterprises and perhaps even the cloud barrier, since the trend is toward cloud data storage.

The solution could be promising new behavior analytics technology that parses the numerous events that occur at lightspeed to find anomalies in normal behavior, hinting a possible invader whose signature is unknown. Leaders in the C-suite need to be aware that there is hope for SMBs who typically cannot afford the protection offered by enterprise solutions. They also need to be cognizant that even large enterprises with their existing sophistication enterprise solutions may not be safe from malware invaders.

Introduction

Malware attackers can be anybody. A hacker doesn't have to be a coder to get their hands on third-party malware these days. This brings the down the sophistication bar previously needed to design an attack mechanism, and it increases the number of bad acting opportunists knocking at your network door.

Pain Points

To date, ransomware victims have been essentially off the grid of the authorities. They are small businesses and healthcare entities that, when faced with a ransomware threat, need to beat the attacker's count-down clock to avoid significant downtown and loss of business. The threat is real. All the attackers want is cash, and once they get it, they quickly unlock the hostage data and disappear into the wind.

The large companies have the resources to invest in today's sophisticated, comprehensive enterprise solutions. That leaves SMBs pursuing point solutions, which, unfortunately typically don't communicate with other security devices and applications. And SMBs often do not have the IT resources and expertise to manage all of the various security solutions in a layered mesh around corporate assets.

A bigger pain point is that current malware solutions are signature-based, meaning that somebody has to get hacked and the code captured and analyzed before a signature is known. With the increasing ease that bad players can now make to malware code – thereby creating unknown signatures - malware vendors are scrambling to get ahead of the problem.

Resolution

Besides improving security hygiene, by applying IT security best practices, and educating their people, the C-suite must amend their security solutions to newer technology that pursues detection of the yet "unknown". That is certainly difficult to do without having access to the code hackers are using.

Two security vendors are pursuing a promising behavior-based technology. This article discusses this technology from two interesting perspectives: RSA, a leader in comprehensive enterprise security solutions and MalwareBytes making waves in malware detection and remediation.

RSA Presents Enterprise Solutions and Managed Services

Peter Tran, GM & Sr. Director, Worldwide Advanced Cyber Defense Practice, RSA and I discussed Ransomware and RSA's approach to managing this problem and expectation of future growth.

Ransomware often attacks small businesses and individuals for small cash rewards. But, as Tran comments, "The stakes are higher for enterprises, such as healthcare, where a hospital being held hostage affects many people in critical care, such as with Hollywood Presbyterian Medical Center." Ransomware is moving beyond preying on only SMB (Small to Medium Businesses). He said it is now run like a business, investing in malware changes and recruiting more bad actors to purchase and distribute malware permutations. This shift is preventing security vendors from being able to keep up with the massive changes.

Tran related, "We are focusing on the analytics of behaviors at the endpoints, before the malware can become weaponized." He added that the context around malware analytics is to establish virtual playgrounds to focus on malware behavior – what it is doing and how it plays. But to be effective, "we need to expand [the view] across the enterprise, not just malware analytics, but how it interacts with machine-to-device, device-to-device, all the way down to the endpoint. [You need to] get a better field of view of what your network may be exposed to." A better risk indicator goes beyond simply recognizing the enterprise hot spots – it must also see how they relate.

A major problem for SMBs in acquiring an enterprise-wide security solution is the required investment. Tran indicates that simply buying a point solution tends to be myopic. “This has always been a quagmire for SMBs,” notes Tran. He says this is where Managed Services is leading – there must be some sort of compromise, where SMBs will purchase a subscription to a security report evolving toward analytics and behavior-based.

As companies push more IT transactions to the cloud, what can we expect from Ransomware and other malware attacks? “The threat to the cloud is not going to stop,” states Tran.

Tran continues to say that the stakeholder(s) of risk management is evolving. Whereas RSA is often briefing company boards on agenda, attitudes are changing. Whereas the consumer of security data has typically been the Director of IT, CISO, or Director of Risk, this information should be circulated to the others in the C-suite, not just the CSO/CISO.

The Solution is more than Just the Technology

Technology by itself is not the solution. Tran emphasizes the importance of following best practices as recommended in RSA’s cybersecurity framework, which is anchored in the White House’s cybersecurity framework under Executive Order 13636, and reflects what the Department of Homeland Security is doing.

Tran notes RSA shares with its customers the importance of “framing” itself, i.e., applying a cybersecurity framework. The business needs to break up its best practices and implementation into the top functional domains, such as the rapid response function, and the content analytics and threat intelligence functions that drive the enterprise’s Core, or what RSA calls the “Operations Core”. Otherwise, the organization simply is functioning in “operational thrashing” mode, where the organization is disorganized and does not know how to consume its security data.

Stakeholders need to break down their best practices into controls that fall under the framework’s functional domains and then incrementally improve that to see how they fall into the security maturity model. The best implementation is based the organization’s response function, content analytics, and threat analysis that drives the “Operation Core”.

NIST and technology training and gamification are important to empowering organizational readiness. According to Tran, “Because Security Analysts work in 12-minute bursts, education of your security people must change from simply using classroom training to encompass gamification and cyber ranges.”

MalwareBytes

One of the big problems with relying on Anti-Virus software alone to protect a business, as is often the case with small businesses, is that the security solution is only as current as the most-recent update. AV vendors are constantly updating their solutions as new malware signatures are identified. Unfortunately, with ransomware, capturing the signature is difficult (since paying the ransom, removes the signature from the infected device before authorities can capture it), and even if it is, it is much easier for bad players to change. This means that the “guardians of security” are always behind what the bad guys are doing.

Adam Kujawa, Head of Malware Intelligence, noted that MalwareBytes is solving the dilemma of guarding against unknown signatures by replacing Anti-Virus software with something better –

behavior-based monitoring and analytics. Kujawa notes, “Of course, this is significant because we can now detect and analyze common endpoint behaviors for traces of anomalies possibly meaning presence of a bad actor.”

MalwareBytes looks at all process activity for what seems unusual. Whereas processes creating new files may be low on the threat scales, processes encrypting files or creating random keys could be something to worry about and investigate further. When a monitored process hits a specific threshold, the security solution kills the process and all its traces. Kujawa adds, “With process injection, MalwareBytes traces back to the executable, and deletes any traces of it.” The idea is to stop the malware vector, and take care of all angles of an infection vector. Malware likes server software because it can quickly deploy while avoiding signature detection and recognition. It can be telemetry sourced.

As with RSA’s Tran, Kujawa believes that ransomware attempted attacks on the cloud are guaranteed to happen. He adds that MalwareBytes is striving to be ahead of the malware curve. Companies need to have a well-planned Disaster Recovery plan, and ensure their back up system is current and working. You want to be prepared, not panicked and reactive, which falls directly into the hands of malware exploiters.

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.

Photo: Jon Leer