Stratecast | FROST & SULLIVAN

September 23, 2016

War on Ransomware

No Silver Bullet Defense, but Indifference is Not an Option Either

Stratecast Analysis by

Michael P. Suby

Stratecast Perspectives & Insight for Executives (SPIE)

Volume 16, Number 34

War on Ransomware

No Silver Bullet Defense, but Indifference is Not an Option Either

Introduction[1]

Ransomware cannot be ignored. It is a malware category that is growing in size and impact. According to McAfee Labs, the number of new ransomware samples has been accelerating significantly over the last four quarters. For the quarter ending June 2016, the number of new ransomware samples was over 1.3 million. Correspondingly, on a year-over-year basis, the total number of ransomware samples increased 128%, reaching over 7 million unique samples.[2,3]

Contributing to this escalation in ransomware are the following:

- **Systematic and scalable malware development is common** – Polymorphic and metamorphic code techniques and easily accessible base code toolkits support the rapid development of ransomware variations/samples.[4] Furthermore, selling ransomware is now a business, as Check Point detailed in its analysis into ransomware-as-a-service.[5]
- **Tried-and-true malware delivery mechanisms continue to be effective** – Even with security training and awareness, there is still a material portion of end users that click on attachments in phishing emails, and visit websites that host drive-by malware. Verizon's data breach investigations provide evidence of this: 30% of phishing messages were opened by the targets (i.e., end users), and 12% of the targets clicked on the malicious attachment or link.[6] Unfortunately, just one compromised endpoint is sufficient for the malware to gain a foothold.
- **Businesses, not just consumers, are affected** – In a 2016 multi-country survey of CIOs, CISOs and IT Directors, sponsored by Malwarebytes, 39% of the represented businesses experienced a ransomware attack; and 37% of the victims paid the ransom demands.[7] Paying

[1] In preparing this report, Stratecast conducted interviews with representatives of the following companies:

- Acalvio Technology – Ram Varadarajan, Co-Founder & CEO; and Raj Gopalakrishna, Co-Founder & VP Architecture
- Attivo Networks – Marc Feghali, Co-founder & VP of Product Management; and Carolyn Crandall, CMO
- Fireglass – Zach Beiser, VP Marketing and Business Development
- Malwarebytes – Pedro Bustamante, VP Technology
- TopSpin Security – Yoel Knoll, VP Marketing; and Rami Mizrahi, VP R&D
- TrapX Security – Anthony James, Chief Marketing Officer

Please note that the insights and opinions expressed in this assessment are those of Stratecast, and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

[2] See *McAfee Labs Threats Reports, September 2016*, page 43.

[3] For a more recent observation, see *Check Point Research Reveals Surge in Ransomware in August* (September 19, 2016).

[4] Two relevant blogs on this topic were developed and posted by Fortinet: *On-Demand Polymorphic Code In Ransomware* (June 6, 2016); and *Metamorphic Code In Ransomware* (January 26, 2016).

[5] See *CerberRing: Ransomware's Underworld An in-depth exposé on Cerber and ransomware-as-a-service* (August 2016).

[6] See *Verizon 2016 Data Breach Investigations Report*, page 18.

[7] See *Understanding the Depth of the Global Ransomware Problem* (August 2016).

a ransom is not the only cost. Other potential costs include: lost productivity, reduced revenue, brand damage, and, as Malwarebytes's survey also showed, remediation effort—63% of attacks took more than nine hours to remediate. For attackers with "success" not only measured by ransom payments, ransomware bolsters attackers' ability to heap supplemental and potentially far greater harm upon their victims.

Given this rising risk of being victimized by ransomware attacks, what should a business do? Realistically, there is no silver bullet to completely eliminate the risk. Rather, a mix of operational best practices and security technologies can have a sizable and sustainable impact on mitigating ransomware risk, and favorably reduce the risk of being victimized by other advanced malware threats as well. In this insight, we discuss approaches to mitigate ransomware risk, and present our opinions on their advantages and limitations. In the process, we will pay particular attention to two security technologies we have discussed in previous insights—namely, isolation and deception—and another security technology that we will be spending increasing attention on in the near future: signature-less endpoint protection.

What Ransomware Is and How it Operates

Simplistically, ransomware is a malware category designed to render digital assets, such as electronic files, unusable through encryption until the victim pays a ransom for the decryption key. Upon payment, frequently with bitcoins, the decryption key is potentially provided to the victim.

With the increase in ransomware samples, how ransomware operates will vary. Even so, the general kill-chain steps are:

- **Distribute** – Ransomware, like other forms of malware, is typically delivered to end users' computers through email attachments and compromised websites. Other distribution means are possible, such as a USB thumb drive, but email and websites are the most common.
- **Execute locally** – The ransomware infects the machine, and execution begins, sometimes immediately; but it also could be triggered by an end-user action or a system operation.
- **Communicate externally** – The ransomware reaches out to an external command & control (C2) server to retrieve an encryption key. Although this approach is the most common, some ransomware variations are pre-loaded with an encryption key.
- **Delete backups and disable restores** – Recognizing that file backups, local and online, can be used to recover from a ransomware attack (i.e., replace ransomware-encrypted files with unaffected backups), some of the more sophisticated ransomware variations will delete backups and disable restoration capabilities.
- **Search** – The ransomware searches for assets to encrypt, typically files and folders, both locally and on network drives.
- **Encrypt** – The files are encrypted. Alternatively, the files are first renamed, then encrypted, and then renamed again to further complicate recovery efforts.
- **Demand ransom** – C2 contact is made and a ransom note is delivered to the victim.
- **Spread** – If one infected machine is good, more are better. The ransomware is spread laterally to other machines, and the process is repeated.

Approaches to Defend Against Ransomware

In this section, we discuss three approaches that insulate businesses from ransomware attacks, and minimize the impact *if* (or maybe better stated as *when*) an infection occurs. Those approaches are:

- Circumvent ransomware distribution
- Containment following infection
- Declaw lateral movement

Our opinions on advantages and limitations concentrate on two attributes: ease-of-use and effectiveness. Ease-of-use is evaluated along two vectors: transparency and effort. Ransomware-defeating approaches that are transparent to end users and administrators (e.g., no material change to their existing workflows and routines required); or, if changes are required, the extent of change or effort is minimal, are viewed more favorably than those that are less transparent and more involved. Effectiveness is also evaluated along two vectors: (1) where in the kill chain the approach occurs, with earlier as preferable; and (2) comprehensiveness (partial or complete detection and prevention). Naturally, both vectors are important. An early kill-chain approach that leaves major attack vulnerabilities exposed would be significantly less effective than an approach that occurs later in the kill-chain but is more comprehensive.

Circumvent Ransomware Distribution

Optimally, stopping initial attempts at distributing ransomware to endpoints is best. It is the ultimate in prevention if it can be both easy-to-use and highly effective; and, of equal importance, does not interfere with business operations. Alas, as described below, no silver bullets here.

End-user Security Training

End users are well-recognized as the weakest link in cybersecurity. Either out of ignorance, laziness, or malice, end users' actions (clicking on malicious attachments and visiting compromised or low reputation websites) open doors for ransomware entry. Not that end-user security training should stop or not begin, but it should be placed in its proper context of reducing but not eliminating these openings.

Web Security and Email Gateways

Situated in-line with the communication freeways, these gateways can stop access to known bad and potentially malicious websites and URLs, and can prevent clicking on suspect email attachments. With web security and email gateways commonly deployed as security technologies, the workflow or operational change in pointing them to ransomware defense is immaterial; just part of the package. The effectiveness of these gateways is, nonetheless, dependent on their accuracy and completeness in identifying compromised websites and attachments that include ransomware, or point to websites that host ransomware. With the number of ransomware variations ramping upward, and the existence of momentary websites and URLs, comprehensiveness in identifying all the bad is more aspirational than realistic.

Integrating with sandboxing technologies for safe denotation and discovery of malicious attachments and website links adds to comprehensiveness, but at the price of potential workflow latency and more security technology to manage. Plus, malware writers are not oblivious to sandboxes, and will wrap their payloads in sandbox-evasion techniques to avoid detection. Even so, the Advanced Malware Sandbox (AMS) market is competitively healthy. The market grew 83% in

2015, to nearly $1 billion—clear evidence that the advanced malware battle cannot wait for a perfect defense, and that enterprise values what AMS solutions deliver.[8]

Remote Isolation

The concept of remote isolation is to execute web and email sessions external to end-user machines, and render benign visualizations of user sessions (i.e., no active links, software code, or attachments). This approach eliminates the question of comprehensive and accurate detection that plagues antivirus/antimalware, next generation firewall, web and email gateways, and network sandboxes, as there is no detection involved. All sessions are executed in remote, individualistic, and temporary containers, typically cloud-based; and all user content is rendered as a safe, inactive visual stream. This approach is also referred to as sanitization.

Designed to be latency-free and preserving of users' mouse and click movements (i.e., look and feel), the end-user experience is undifferentiated from local browsers and email clients. For IT and security administrators, the beneficial promise is a narrowing in policy management, fewer access-permission confrontations with end users, and, ultimately, fewer infected endpoints to clean or reimage.

The competitive marketplace for this security category is not as wide or as mature as other security technology markets. Two notable suppliers making market headway are Menlo Security and Fireglass.[9] Additionally, and a potential signal of an upcoming path-to-mainstream, Check Point has partner integrations with both of these companies; and, separately, through its own development, offers document sanitization with its Threat Extraction blade.

Remote isolation, despite its promising capabilities, is not an all-encompassing solution, either, in the battle with ransomware. Deactivating or sanitizing content may not cover all distribution channels, as the current solutions focus on web, email, or web and email channels. Ransomware delivered through other means—for example, USB thumb drives, sanctioned cloud or appliance-based file share and synch systems, and unmanaged network-connected devices (e.g., bring your own devices)—could still be avenues for the delivery of ransomware and other advanced forms of malware.

Containment Following Infection

With no one approach providing 100% certainty that all ransomware will be blocked from landing on endpoints, the next stage of defense is to contain the infection. Here too, there are multiple approaches.

Good IT and Security Hygiene

In an empirical study on ransomware mitigation strategies produced by CyberArk Labs, this organization found that a combination of removing local administrator rights on endpoints, and practicing application greylisting (a combination of application whitelisting and blacklisting) was 100% effective in blocking ransomware from gaining the necessary permissions to access and

[8] For a thorough analysis of the Advanced Malware Sandbox market and suppliers, click on Frost & Sullivan's *Advanced Malware Sandbox Market Analysis -"Must Have" Security Technology Reaches Mass Adoption* (September 2016).

[9] We profiled Menlo Security in this insight: *Defeating Malware: Isolate and Sanitize Rather than Detect* (July 2015).

encrypt protected file types. To arrive at this result, CyberArk created a production environment and trialed several strategies to defeat a varied set of 23,000 ransomware samples.[10]

While an admirable outcome, these strategies should, as CyberArk logically notes, already be standard IT best practices. But with ransomware attacks having a 40% infection rate (Malwarebytes survey), and countless security companies rushing in to promote their solutions as a means to defend against ransomware attacks (another indicator of the aggravation ransomware is causing), either these best practices are not followed routinely or only partially, or the test environment could not account for all the potential environmental conditions or ransomware samples, to extrapolate this outcome universally. Also, as we are not in a position to technically critique CyberArk's test, we suspect that a primary contributor to the continuing success of ransomware attacks is that these and other best practices are not followed thoroughly, due to lack of discipline or unique business circumstances and constraints. Thus, we reach a similar conclusion as we did with end-user security training: following these best practices is highly recommended, but should not be considered a 100% failsafe approach in practice.

Detect and Prevent at the Endpoints

With user endpoints being the location that ransomware initially lands and executes, placing defenses in this same location is only logical—that is, prevention at the point of infection. Not only can this defensive location protect local hard drive files from being encrypted by the ransomware, but will also be a critical line of defense in blocking ransomware encryption of files in network drives, and prevent ransomware propagation to other endpoints.

Challenging in this strategy is that traditional endpoint security, such as antivirus/anti-malware (AV), cannot keep pace with the rapid development of ransomware. McAfee, as previously noted, identified over 14,000 new ransomware samples per day during the three month period of April – June 2016. This pace challenge is not new with signature-based (also referred to as pattern matching) endpoint security products. The process of identifying, analyzing, and creating signatures for new pieces of malware takes time, and so does distributing new signatures to the endpoints. With ransomware, any time delay, however, is a window of opportunity, as file encryption could execute immediately after the endpoint is infected. By the time the new signature is created and distributed, the damage may already be done, and the victim is forced to pivot from prevention to recovery (i.e., paying the ransom or retrieving backup files, if they exist).

Even though traditional endpoint security products are challenged to combat all zero-day ransomware attacks (i.e., previously unseen samples), these products still materially reduce the attack surface by purging known ransomware signatures from endpoints. Since attackers are resourceful and frugal, they use older, lower-cost ransomware variations in hopes of infecting "weakly protected" endpoints. Plus, traditional AV is woven into most businesses' desktop management workflows. So, even though not 100% effective, traditional AV remains an established and valuable component of a ransomware defense strategy.

With signature-dependent defenses being inadequate in protecting endpoints from ransomware, the logical complement is signature-less endpoint protection. AV vendors, large and small, have been active in this approach for some time. One company we call out in this report is Malwarebytes. It has a multi-prong strategy for combating ransomware at the endpoint, and has a solid tenure in endpoint remediation (frequently running side-by-side with traditional AV products

[10] See CyberArk Labs, *Analyzing Ransomware and Potential Mitigation Strategies* (August 2016).

to remove all artifacts of an infection). According to the company, it is experiencing accelerating market uptake in the small and midsize business segment, which it entered in 2012; and in the enterprise segment, which it entered in 2015. Also, the Malwarebytes protection strategy is designed to combat the more sophisticated ransomware variations by circumventing their activities and exploits that precede file encryption (early warning and intervention), as well as when encryption is attempted. Last, with the exception of a few dedicated features for combating ransomware, the company's protection strategy was designed to circumvent a range of advanced attack methods.

Malwarebytes' endpoint protection strategy includes the following components to address each stage of an attack:

- **Profiling** – Ransomware authors will seek to profile the environment to assess defenses and vulnerabilities. Without the use of rules-based signatures, Malwarebytes blocks this reconnaissance activity emanating from sources like malicious advertisements hosted on trusted websites.
- **Delivery** – With a toehold on the endpoint, communication will be attempted with an exploit server to retrieve the ransomware exploit kit. Armed with an evergreen library, Malwarebytes stops these communication sessions from initiating.
- **Exploitation** – Also signature-less, Malwarebytes detects and blocks attempts to exploit endpoint vulnerabilities, and remotely execute code on the endpoint.
- **Payload execution** – As an alternative to traditional AV, Malwarebytes disrupts malware payload execution as it attempts to force sanctioned applications to behave inappropriately (signature-less); and uses heuristics and behavioral rules (signature-based) to identify and remove entire known ransomware families (e.g., CryptoLocker).
- **Malicious behavior** – As the final layer of defense in this attack chain, Malwarebytes uses proprietary behavior monitoring technology to block local file encryption. Communication with command & control servers and malicious websites is also blocked (signature-based).
- **Remediation** – True to its tradition, Malwarebytes removes the active components of the ransomware infection and all related artifacts.

Endpoint protection of the signature-less variety is gaining market momentum. Competitively, newer vendors sense opportunity to shift market share away from the incumbents, and the incumbents are not blind to this aggressiveness. In turn, these two factions will spur higher levels of innovation, price and feature competition, and greater customer choice. The beneficiaries will be the buyers.

Declaw Lateral Movement

The predictable evolution of ransomware is that, with success, cybercriminals will pursue higher value targets to attain higher ransom rewards. Disabling or encrypting the files and backups of an endpoint will no longer be financially satisfying. Cybercriminals will apply the capabilities developed and experiences gained in targeting endpoints, and target a wider variety of network-connected assets, particularly those that are instrumental to critical, business-dependent operations. This evolution is, to some extent, already underway. McAfee Labs, in its research, noted 20 hospitals that

were victims of ransomware attacks in the first half of 2016.[11] Furthermore, the affected assets were not just end-user endpoints, but also included servers and medical devices, like MRI machines. These are assets that required the ransomware to snake laterally through the organization's network to reach.

In another telling aspect of the costly pain felt by the victims are the non-ransom costs, as we noted previously, but also noted by McAfee Labs:

> *"The biggest direct costs [of a ransomware attack] were from downtime (lost revenue), incident response, system recovery, audit services, and other cleanup costs. In the reports we reviewed, healthcare providers were at least partially down for five to 10 days."*

With lateral network movement to take control of high-value assets representing another vulnerability vector that ransomware exploits, what should businesses do in response? Beneficially, there are viable defenses. Deception products, for example, were explicitly designed to mitigate this lateral movement vulnerability, caused by advanced malware as well as malicious insiders. Deception, however, is not the only means to lessen this vulnerability. Application whitelisting, network segmentation, and air gapping are other vulnerability-lessening means; but these other means may not always be feasible. An alternative or complementary means may well be in order when critical assets are in attackers' sights.

As described in a recent Stratecast insight, deception consists of two primary components: (1) breadcrumbs/lures and (2) deception decoys.[12] Pertaining to advanced malware, the breadcrumbs are attractive pieces of fake information (e.g., user, application, and browser credentials; and server message block (SMB) network share tokens) hosted in endpoints. The malware gathers this information, and with it, is lured into the deception decoys. These decoys, virtual representations of genuine assets (e.g., network file shares, servers, and IoT devices), interact with the malware. In theory, these interactions captivate the malware and counter the malware's programmed instinct to pursue real assets. Through this interaction with the decoys, infected endpoints are immediately identified; high-fidelity forensics on the malware tactics, techniques, and procedures (TTP) are catalogued; and incident responses are triggered (e.g., disconnecting the infected endpoint from the network, and launching scans to locate and remediate other infected endpoints).

In detecting and engaging ransomware, a common approach is to place fake SMB network share tokens on endpoints, with the tokens pointing to network share decoys. To be effective, deception products are, at minimum, proficient in the attributes of authenticity, automation, and adaptation. While differentiation in these attributes across vendors exists, other product features also exist to extenuate detection and inoculation of ransomware. Following are examples:

- **Attivo Networks** – Among the most tenured deception companies in the market, with its continuous threat management platform, the company has further enhanced its platform with the recent introduction of ThreatPath. ThreatPath combines detailed information of customers' systems with intelligence on advanced malware TTPs, to create highly customized incident prevention blueprints.
- **TrapX Security** – Specializing in emulation, the company positions itself to rapidly emulate a wide range of device types; in particular, medical devices.

[11] See *McAfee Labs Threats Reports, September 2016*, pages 24-25.

[12] See *Deception as a Security Discipline - Going on the Offensive in the Cybersecurity Battlefield* (July 2016).

- **TopSpin Security** – Utilizes continuous monitoring of network traffic and sniffing of egresses, combined with sophisticated correlation techniques to detect ransomware early in its post-infection executions.
- **Acalvio Technology** – Soon to enter the market, this vendor inserts itself into multiple stages of the ransomware kill chain. As an example, the company deploys honey emails to clandestinely attract phishing schemes.

The wave of deception products is relatively new; accordingly, mainstream confirmation of effectiveness in defending against ransomware is not yet present. Plus, these products are not positioned as improved alternatives to existing security solutions. Consequently, they represent an added expense and management responsibility. Nevertheless, deception provides a conceptually innovative means to reduce the risk of advanced malware, such as ransomware, in moving laterally through an organization's system, and causing greater damage.

Stratecast
The Last Word

Ransomware is not a new exploit; it has existed for more than a decade. Likewise, the fundamentals of ransomware have been relatively unchanged over the years. What is different now are the circumstances. Those changed circumstances include:

- The means for creating new variations is more industrialized
- Cybercriminals are more organized; this "business" has evolved from blue to white collar
- Ransom payment methods have transformed from a briefcase of bills to a faceless, virtually untraceable electronic transaction
- More people, in both their personal and professional affairs, spend more time connected and interacting with systems and applications; and this contributes to the steady transformation of the bloodstream and archives of life from physical to electronic

Bundling these changed circumstances together, the means and motive of ransomware has ratcheted upward. Yet, many of the same protection techniques and technologies that existed a decade ago are still in use today. While there have been updates and advancements in protection, as well next-gen additions, there has also been an uptick in exploits and being exploitable.

This rise in ransomware is a bright demonstration that *how* security is practiced is inadequate. Change is needed. A return to IT and security best practices is overdue, and should be undertaken even if this return impacts business agility. Business will adapt; it always does. Also, a retooling of the security infrastructure is needed, to approaches that deliver greater outcome certainty and adhere to a more holistic "follow the kill chain" design. The sample approaches we called out in this insight—remote isolation, comprehensive endpoint protection, and deception—are representative indicators that innovation in security holds promise in altering the status quo of becoming a victim.

Michael P. Suby

VP of Research

Stratecast | Frost & Sullivan

msuby@stratecast.com

About Stratecast

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.