Scourges of the Modern Endpoint: Keeping Your Eye on the Bigger Picture

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper

Prepared for Malwarebytes

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

SCOURGES OF THE MODERN ENDPOINT: KEEPING YOUR EYE ON THE BIGGER PICTURE

Table of Contents

SCOURGES OF THE MODERN ENDPOINT: KEEPING YOUR EYE ON THE BIGGER PICTURE

Introduction

Millions of dollars are being spent by crime syndicates and other organizations to create malware, to steal billions of dollars from enterprises and consumers. For them, it's a great racket, for the rest of the world it is a significant resource burden. There are many forms of malware each with its own forte. The most recent class to take off and gain the limelight is ransomware but before that were a myriad of other types of malware that IT and security teams have been challenged by for years. While there are three to four dozen versions of ransomware, there are literally millions of versions of malware.

Though the current media hype focuses on ransomware, and it is indeed a problem to be reckoned with, there are multiple factors to be considered when researching endpoint defense and making security program decisions.

Ransomware is Bad (As if You Didn't Know…)

The State of Ransomware

Ransomware flourished in the last few years due to the convergence of three factors. The first was the expansion of public key cryptography. Granted, this expansion has been around for more than 20 years, but it was the first of the three factors to emerge. The second was the increase in processing power and memory for common PCs. As common PCs amped up, they could perform many asymmetric crypto operations in the background without significant impact to the user, who was unaware that the ransomware was deployed and decrypting files. The final factor to thriving ransomware was a simple, irrevocable, and untraceable payment method. Attempts to exploit a payment method up to that point were often met with disappointment. Cash and checks took too long to deliver, checks could be cancelled, and credit cards were faster, but those transactions could be also be cancelled. Also, the large issuers had international connections and after enough financial pain, could motivate local law enforcement in the recipient's domain to act. Wire transfers were more timely and direct, but they were not timely enough and also left some financial breadcrumbs to give away information about the recipient that might be useable for warrants and future prosecution. The right method was needed, and that method appeared and gained momentum in the form of BitCoin Cryptocurrency. It created value and was untraceable in the normal financial machine. A person could be directed where and how to buy BitCoin Cryptocurrency on the web, so it combined speed, non-traceability, and non-revocability in one fell swoop.

The evolution of ransomware relied on faster processors, wide availability of asymmetric cryptography, and untraceable, irrevocable payments.

Ransomware: The Single-Trick Pony

Though there are literally dozens of ransomware variants (some very successful and others not so successful), they all are similar in their approach and the same in their objective and successful outcome. They all rely on some form of delivery method, an exploitation method to start working on the system, and asymmetric cryptography. Whether delivered through a phishing email, a malicious website, or a Trojan program, once on the system, ransomware exploits a vulnerability against the operating system or the user's identity and then begins encrypting files. Most PCs use AES with a 256-bit public encryption key to render files inaccessible. The attacker keeps the private key safely stored on a command and control server until payment is received.

Ransomware is Damaging but Meant to be Detected

At some point in the encryption process, usually closer to the end, the ransomware intentionally alerts the user to its presence. This must happen in order to start the payment process. Ransomware gets in the user's face to tell the user what it has been up to, that there is no hope other than payment, the amount of ransom demanded, how to contact the attacker to deliver payment, and where to get the decryption key to reverse the process. Ransomware attackers do not want to leave any guesswork, because that impacts the amount of revenue they collect.

Costs of Ransomware

Ransomware has made its mark on the world. Back in 2015, each consumer ransomware attack averaged about $300 USD. However, in 2017, that average increased to just over $1000 USD.[1] Successful attacks in a professional environment can be significantly higher, demanding tens of thousands of dollars per incident. Each of these incidents combined brought estimated revenues in 2015 to about $325 million USD. By the end of 2017, it is expected to have achieved more than 15x—reaching over $5 billion USD.[2]

Aside from the ransom there are costs for business disruption of the person or people affected and if ransom is not paid there are administrative costs for restoring data from most recent backups. Inevitably this also leads to some data loss as very few backups have every bit of data.

As Bad as Ransomware is, Other Malware is Worse

In the fervor to address the ransomware threat, people seem to have almost forgotten that there are literally millions of other strains of malware in the wild waiting to pounce on them with the wrong click of a button.

Malware uses essentially the same delivery methods as ransomware and, though the goal of these other forms is most often to create revenue for the authors and attackers, the method is usually not to directly extort cash. The way they go about making money for their authors is often very different.

While ransomware is "in your face" about its intent, other malware relies on stealth and can therefore exact a much higher toll over its lifecycle.

Stealthy Nature

First, outside of the ransomware family, effective malware is stealthy. Malware relies on stealth and therefore malware authors go to great lengths to make it that way. It does not want users to detect it because the greater its dwell time on the host, the more data it can collect and the deeper it can infiltrate an environment to get closer to its target. Malware makes more money for the attacker when it remains hidden! This is why there was a billion-dollar industry devoted to detecting and preventing malware well before ransomware became an issue.

1 Average Ransomware Demands
2 Ransomware Damage Report

General Categories of Malware

Malware that gains revenue directly. Aside from ransomware, other types of malware falling into this category are RAM scrapers, keyloggers, financial trojans, adware and other pop-up programs, some forms of bots, and spyware. In this context, malware is most often interacts with the user's browser to create pop-up advertisements or pretending to be the user to produce click fraud which defrauds advertisers into thinking their ads are being investigated by an interested party so they pay the fraudster for those clicks. RAM scrapers, keyloggers, and financial trojans can provide direct revenue by collecting user credentials, allowing the attacker access to financial and credit accounts.

Malware that gains revenue indirectly. Keyloggers, remote access Trojans (RATs) and other generic Trojan programs, RAM scrapers, bots, rootkits, and backdoors all gain revenue indirectly by giving the attacker some level of access into the user's system and/or web accounts. Where no direct financial accounts are acquired or desired, access to the accounts and systems can then be leveraged as a traded commodity or provide the attacker with means to collect other information that can then be used or sold. Bots are rented or sold to be used in denial of service or other forms of attacks.

Denial of service malware. Common "traditional" viruses, bots, and worms are often used to create a denial of service situations on the infected host. In the cases where a single end system is impacted, there is seldom revenue involved. In the case of bots, those are controlled in collectives known as bot nets, which can be rented out as a service.

Business Impacts

Commercial intellectual property (IP) theft is skyrocketing. Poster children for the magnitude of these losses include names like Nortel, American Superconductor, and Sony Entertainment. Nortel had hackers siphoning out and selling its IP for years, allowing the overseas competitors to gain market share without the research investments. American Superconductor IP was stolen by a malicious insider and sold to an overseas company, dropping its stock shares by 90 percent. Sony Entertainment suffered brand and reputation damage and incurred over $35 million USD in cleanup and estimated its IP losses at over $100 million USD. Many other individuals and companies have been similarly impacted.

EMA Perspective

Don't Lose Focus on the Broader Threat

While ransomware is undeniably a big hitter, its overall impact is a mere drop in the bucket compared to the rest of the body of malware. Looking at the cost of losses from ransomware, both direct and indirect, the number mentioned earlier was about $5 billion USD. Even after removing the current $5 billion from the pot, the cost of malware-related losses[3] three years ago in 2014 was over $486 billion dollars. That is nearly 100x or two orders of magnitude larger than the current malware threat, or 9720 percent more of a financial impact.[4]

It's entirely a game of numbers. The larger pool of malware out there and a diverse goal set for its use puts other malware at far greater market saturation than ransomware. It also means the other malware is not going

While ransomware cost the world about $5 billion USD, other forms of malware cost the world 9720% or nearly 100x more!

3 Financial Costs Incurred by Malware Incidents
4 Breaches Cost Study

to go away anytime soon. So, while consumers should be ever vigilant against ransomware, they must not forget why the whole industry of endpoint protection was started and that the threats they are dealing with are diverse, stealthy, and prolific.

As consumers considered a solution to protect their personal endpoints, they turned to Malwarebytes to find and resolve the threats that traditional antivirus failed to detect and prevent. Now, Malwarebytes is available at an enterprise scale with even more advanced technology to detect and prevent malware of all types.

About Malwarebytes

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts. For more information, please visit us at http://www.malwarebytes.com/.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3712.092217