Protecting against Tomorrow's Malware Attacks Today

By Guy Bunker – ISSA member, UK Chapter

This article discusses why cybersecurity organizations need to rethink how they protect against the next wave of malware attacks and information-borne threats.

Abstract

This article discusses why cybersecurity organizations need to rethink how they protect against the next wave of malware attacks and information-borne threats. The author analyzes monetization strategies driving malware development, the latest social engineering and payload delivery techniques, and a layer of sanitization to detect and prevent an attack before it starts.

It's always difficult to hit a moving target or prepare for the unexpected, but proactively securing your organization's critical resources from tomorrow's ever-advancing malware attacks can seem daunting to the point of being unsustainable. Cybercriminals and rogue nations are not only evolving their malware attacks by relentlessly developing sophisticated social engineering and payload delivery techniques, but are shifting who and what is being targeted and how their attack will be exploited or monetized. The game has changed, and so must the approach cybersecurity leaders take to protect against the next generation of malware attacks from bypassing their perimeter defenses and threatening critical infrastructure and sensitive information.

Anatomical evolution

The evolution of malware attacks has been heavily influenced by the end game for the cybercriminal. How will the attack be monetized or exploited such as the case with hacktivism or espionage? While there are still illegal profits generated by extracting sensitive information from organizations to be sold on the dark web's black market, it is being heavily reported that there is a shift in value and priority from traditional personal identification details such as social security and payment card numbers to more prized medical record information and intellectual property. In fact, Reuters has reported that medical information is now worth 10 times more than credit cards.[1] And according to CNBC, the demand for stolen information for consumers centers around PayPal, Uber, and Netflix accounts. [2]

A more brazen monetization strategy catching headlines due its significant impact on critical infrastructure and the well-being of a large number of people has been the surge in ransomware. Ransomware was limited to the consumer market, but is now becoming increasingly prevalent in the commercial space. It was advanced forms of ransomware that were blamed for the havoc caused on Israel's power grid and the locking of patient medical information at a prominent hospital in Hollywood, California.[3] Once systems or data are made inaccessible through locking encryption technologies, cybercriminals demand a high-dollar ransom in exchange for their release. It's these attack outcomes that influence—and will continue to influence—the development road map of tomorrow's malware.

In addition to shifts in malware outcomes, cybercriminals are enhancing their social engineering efforts to more effectively invite themselves behind an organization's defense. Informa-

1 Humer, Caroline and Jim FInkle. "Your Medical Record is Worth More to Hackers Than Your Credit Card." *Reuters*, Thomas Reuters. 24 September 2014 – http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

2 Taylor, Harriet. "Swiped Uber Accounts Worth More Than Credit Cards to Cyber Crooks." *NBC News Digital*, NBCUniversal Media, LLC. 4 April 2014 –http://www.nbcnews.com/tech/security/stolen-uber-accounts-worth-more-stolen-credit-cards-n499796.

3 Murgia, Mudhumita. "Cyber-blackmailers Are Coming for Hospitals, Power Grids and Universities." *The Telegraph*, Telegraph Media Group Limited. 17 March 2016 – http://www.telegraph.co.uk/technology/2016/03/17/cyber-blackmailers-are-coming-for-hospitals-power-grids-and-univ/.

tion harvesting campaigns exploit sensitive data overshared by employees on social media or even from the corporate website. This is not about the obvious details found on the website, but the information that can be harvested from the metadata in the documents posted for public consumption.

Information can be harvested from the metadata in the documents posted for public consumption.

When documents are created, additional information is automatically stored in the metadata in the document. This often contains the author's name, and sometimes even the corporate login name. Further information can be found relating to departments and even system or printer names. There are a number of open-source utilities that can automatically download documents from a public-facing website and then extract and analyze the metadata, revealing the potential threats they contain.

Payload delivery methods have morphed as well, which frequently means new malware variants often go undetected and pass by traditional hygiene and scanning solutions. The more recent delivery methods include the embedding of malicious scripts in a concatenation of multiple business-friendly email attachments, activity hijacking from mirrored versions of legitimate apps or reputable websites, and the modification of USB firmware.

For instance, recently hackers have caused disruption in Ukraine by using spear phishing emails that contain malicious XLS files, the same technique used by the Sandworm group in past attacks. The XLS file tricks the recipient into ignoring security warnings by stating that it was created in newer versions of Microsoft Office and then delivering its malware payload.[4] We've also seen a resurgence of malware in email, specifically malware embedded in email attachments. This threat is particularly potent, as unsuspecting recipients can be vessels for threats and can spread malware throughout their organization simply by trying to open a document.

Additionally, USB sticks can be reprogrammed[5] to imitate a keyboard in terms of issuing commands, mimicking a network card, and redirecting a company's Internet connection by changing the DNS or infecting a computer's operating system prior to booting up, all with the aim of compromising and leaking critical information.[6]

This is very concerning for organizations looking to protect confidential data/information. Malware like BlackEnergy, Dridex, and Locky that use these more advanced delivery methods have recently been plaguing the financial and energy industries by stealing credentials and personal information, causing much stress for both the organizations and their clients.[7] [8] Part of the problem is a reliance on traditional an-

4 Murdock, Jason. "Ukraine Power Grid Attacks Continue but BlackEnergy Malware Ruled Out." *V3.co.uk* Incisive Business Media Limited. 21 Jan 2016 – http://www.v3.co.uk/v3-uk/news/2440469/ukraine-investigating-suspected-russian-cyber-attack-on-power-grid.

5 USB Switchblade. Hack5, LLC – https://hak5.org/usb-switchblade.

6 "USBs: The Inconspicuous Enemy" *Clearswift Blog*, Clearswift. 8 February 2016 – https://www.clearswift.com/blog/2016/02/08/usbs-inconspicuous-enemy.

7 Metzger, Max "BlackEnergy Now Using Word Documents." *SC Magazine*, Haymarket Media Inc. 2 February 2016 – http://www.scmagazineuk.com/blackenergy-now-using-word-documents/article/470225/.

8 Kirk, Jermey. "Locky' Ransomware, which Infects Like Dridex, Hits the Unlucky." *CSO*, CXO Media 17 February 2016 – http://www.pcworld.com/article/3033886/locky-ransomware-which-infects-like-dridex-hits-the-unlucky.html.

tivirus hygiene scanning technologies and filters. These may block some basic embedded threats, but they don't inspect deep enough to detect malware embedded in multiple layers of attached documents and advanced scripting techniques.[9]

Malware prevention tactics

In the past antivirus (AV) solutions were a great way to combat malware; however, today they have become less effective. This is due to the advance of targeted malware that is "unique" or has very few instances for an AV solution to detect. AV is based upon seeing multiple instances of the same malware, often a million times over, and then creating a signature to detect and therefore block it. Without the quantity it becomes difficult to spot. But don't remove your AV solution (!)—it is still very effective against millions of other viruses. However, with AV being ineffective against new targeted malware, a different approach was needed—*introducing the sandbox*.

Today's malware is becoming increasingly sophisticated, and while even a few years ago sandboxing was hoped to solve the problems associated with embedded malware, the malware has become smart—and so the technology is far less effective than it was. Sandboxing relies upon opening a document (or application) in a restricted environment, a sandbox, and then watching the behavior. If it tries to connect to a known bad site, then it can be blocked. Unfortunately, the malware can now take the methods to detect it into account and can hide itself from detection. One of the simplest methods is to wait…and wait. Sandbox solutions typically test for about 15 minutes; after this time the business is more important so the message will be sent on. A simple wait by the malware for 30 minutes can defeat the sandbox. A next generation of sandbox technologies is being developed, but it is simpler to assume that there will be a compromise at some point; therefore, it should be removed before the active content creates an issue. A new approach is needed—*sanitization*.

Deep content inspection (DCI) is the key technology behind sanitization. This is where a document (or an email or web page) is deconstructed into its constituent parts which can then be further analyzed. It is not just about understanding the text that is visible; it is also about being able to distinguish a header from a footer from a watermark. Today's documents have a wealth of information "hidden" inside of them, from the document properties through to revision history and then to "fast save" and active content that could be malware. Tomorrow's malware attacks exploit the complexity of documents today. A deep understanding of the makeup of the document enables advanced solutions to remove the threat, protecting the organization.

Structural sanitization

The most effective way to thoroughly sanitize communications or documents and ensure they are cleansed and safe

9 TECH ALERT: New Email Embedded Malware Getting through Major AV Scans." *Clearswift Blog*, Clearswift. 15 December 2015 – https://www.clearswift.com/blog/2015/12/14/tech-alert-new-email-embedded-malware-getting-through-major-av-scans.

from embedded malware is to add a layer of structural sanitization technology to your existing email- or web-security solution. Structural sanitization leverages DCI to completely disassemble all messages and attachments at a much more granular level to detect and automatically strip hidden and active content. Structural sanitization takes only milliseconds as opposed to sandboxing which can take significantly longer. In a time-critical global marketplace getting the information as quickly and securely as possible has become an imperative.

The active content can be in the form of embedded malware-triggered executables, scripts, or macros such as VBA macros from Office documents, JavaScript, VBScript and ActiveX from HTML message bodies and HTML attachments, and JavaScript and ActiveX from PDF documents. As a result, the malware not caught by standard and AV hygiene scanning and web filters can be completely removed. For today's threats, structural sanitization is cost-effective and can be quickly added to existing email security solutions, protecting your on-premise or cloud-hosted email (i.e., Microsoft Office 365, Google Gmail, etc.) without having to "rip and replace" and provides the most comprehensive defense against ever-evolving email embedded malware.

Document sanitization

While detecting and extinguishing active malware used in an attack is critical, preventing the initial social engineering targeting can help avoid the attack altogether. Fortunately the next generation of adaptive security technology can enable the sanitization of documents automatically—and consistently.

Document sanitization technology thoroughly scans each document being sent through email, uploaded to cloud storage, or posted to the Web by removing all sensitive and hidden metadata used to formulate an attack, leaving the rest of the content and business activity untouched and continuing unhindered. It can also remove revision history and fast-save information, which is another source of data leaks, with a number of high-profile incidents having made the news recently.[10]

Of course, there are a several legitimate reasons to share both metadata and revision history, particularly when collaborating on a specific project. An adaptive solution that can understand the context of the sharing can ensure the correct behavior given the recipient—removing the metadata in one instance, but keeping it in another.

But the system always makes a mistake?

Traditional DLP has suffered from "'the false positive," where communication is blocked due to overzealous policies. The same can be true with sanitization. There are lots of legitimate business reasons to have metadata and revision history in a document and to have macros as well. Today's solutions need to be all about the security, but also need to be about usability—if it isn't usable, then workarounds will happen that circumvent the security measures. Today, context is everything and that is where people are still better than machines. Legacy IT solutions have relied upon the IT department to resolve security issues, and there is still a huge need for that, but when it comes to understanding the business, it should not be individuals in IT who make the decisions. Using document and structural sanitization needs to be coupled with distributed operational administration, whereby the manager (as well as IT and/or the sender/recipient) can be informed of policy violations and help in making the corrective action.

10 Mason, Rowena and Watt, Nicholas. "Small Business Owners' Letter in Telegraph Was Orchestrated by Tories" *Guardian News and Media Limited*, 27 April 2015 – http://www.theguardian.com/politics/2015/apr/27/small-business-owners-letter-telegraph-conservative-party.

Security solutions that understand directory services, for example Active Directory or LDAP, could enable the application to route the alert to the right person who can most effectively deal with it.

Systems will make mistakes; the key is to minimize the impact—and always keep the organization secure.

Protecting from malware now and in the future

While today's threats come in one form, tomorrow's may come in another. It's important for IT departments to be up to speed on the current nature of threats in order to combat them effectively, and choose the right technology for the organization.

When enhancing a malware protection strategy to protect against future threats, it is important to consider:

- Leveraging structural sanitization to remove malicious code from entering your network
- Preventing initial targeting from phishing by sanitizing documents, removing metadata and revision history information before it leaves the organization
- Deploying a second AV on secure email gateways to provide an extra layer of hygiene
- Setting up a sandbox environment for behavior analysis and testing rare cases of required active content
- Tracking and tracing your sensitive information being shared inside and outside the organization with information governance technology

Other ways you can protect your organization from threats is to give staff regular trainings and updates to make sure they can spot malicious threats and avoid putting critical information at risk. A recent survey shows that 88 percent of organizations have experienced a breach in the last year, and only 27 percent of those incidents came from external sources.[11] Your responsibility for information also extends to those you entrust with it. Ensure that they protect your information at least as well as you do.

You need to protect your organization and your information in three fundamental ways, but there is no single silver bullet to do this:

1. **Prevent the bad stuff from coming in.** To the usual boundary protection, add more layers with additional AV and structural sanitization solutions. Consider a sandbox environment.
2. **Monitor inside your network for the effects of malware and advanced persistent threats (APTs).** Deploy effective USB and removable media protection.
3. **Prevent the good stuff from going out.** Deploy a data loss prevention (DLP) solution that can address the traditional DLP functionality, but can also offer next-generation protection with functionality like document sanitization.

The goal of improving your security posture, and in particular #3, is to ensure that if malware successfully penetrates the network, it can't leave with any critical information.

Continued diligence on the part of IT is always required; however, there is a renewed urgency to keep up-to-date on new cyber threats and the solutions that can mitigate them. Ensure you are able to protect your organization by deploying the right solutions.

About the Author

Dr. Guy Bunker, SVP of Products at Clearswift, is an internationally renowned IT expert with over 20 years experience in information security and IT management. Before joining Clearswift, Guy was a Global Security Architect for HP, and Chief Scientist for Symantec. He is a spokesperson for The Open Group's Jericho Forum and an expert for the European Network and Information Security Agency (ENISA). He may be reached at Guy.Bunker@Clearswift.com.

WIS SIG continued from page 9

nesses alike are willing to invest in the talent necessary to keep their systems secure and functional. While not every organization has the need for a dedicated malware analyst or engineer, many large enterprises, consulting firms, government entities and companies specializing in threat-prevention platforms are all competing for the top talent in the field.

As demand continues to outstrip supply in the cyber labor market, we will continue to see increased focus on how to get the right cyber talent into the right positions at all levels. Paired with the evolution of malware, it will take a great deal of creative thinking on the part of companies and governments worldwide to mitigate these increasingly complex threats. Thankfully, there is ample opportunity for anyone curious about a career in information security and a penchant for stopping cybercrime in it's tracks!

About the Author

Domini Clark is the Principal for Blackmere Consulting, an executive search firm dedicated to the information security industry. With over 15 years as an executive recruiter, she has successfully represented Fortune 100 companies, information security services organizations, and technology firms to find, recruit, hire, and retain top level information security talent. She may be reached at domini@infosecconnect.com.

11 Research Shows Businesses Not Prioritizing Growing Insider Security Threat," *Campus Safety Magazine*. 20 March 2015 –http://www.campussafetymagazine.com/article/research_businesses_not_prioritizing_growing_insider_security_threat.