Malware Defense for Today and the Future

This white paper describes strategies for building an effective long-term defense against malware and other threats.
Malware Defense for Today and the Future

Strategies for Building an Effective Long-Term Defense

Introduction

Since the early 1980s, malware has been causing computer and network issues. Despite the billions of dollars spent annually combating and remediating malware, infections and compromises still persist. State and local governments are prime targets for malware attacks. Facing millions of malware variants, with more coming daily, state and local government security teams must not only invest in dedicated anti-malware products, but also leverage every tool in their arsenal capable of helping combat the problem. In this paper, we will provide insights into the current state of affairs and map out the threat landscape with the intent of strengthening your organization’s malware defenses.

What’s driving malware proliferation?

In May of 2014, Tenable Network Security examined malware’s journey from being coded as a hobby to a profit-driven enterprise.¹ In that evaluation, we explored how virtually every piece of malware that is released today has some type of profit motive behind it, whether through corporate or state-sponsored espionage, or more mundane acts of digital extortion or theft. For example, malware developed to collect email addresses is profitable because there is a global market for known good email lists.

Since malware is driven by profit, malware authors are incentivized to perform QA testing on their creations prior to release. In addition to validating performance, this process often includes checking against anti-virus products to see if the new malware is detected.

One of the last things malware authors want is for their creations to provide mass communications. It was quickly realized by both the attackers and defenders that the more “noise” a piece of malware makes, the faster it will be discovered and dealt with (think how quickly LoveLetter² came to the attention of the world). To that end, malware authors have rediscovered the trick of polymorphism. In the modern itineration, the mutation is done on the server side, as opposed to on the compromised host. This allows each hostile binary to have a separate signature, thus increasing the difficulty in detection.

Based on trending data, anti-virus vendors are reporting that “ransomware” has increased 500% in 2013³, and the threat of ransomware has migrated from PCs to mobile devices. Malware such as CryptoLocker made headlines in 2013, but security vendors are also releasing information on how to “safe boot” mobile devices. This threat has become so prevalent, that it has been covered in mainstream business press, such as Forbes Online⁴.

In the field of theft, during the most recent holiday season we saw major headlines concerning data breaches. Multiple retailers had their Point of Sale (POS) systems compromised, and malware such as POSRAM, which concerns the retail sector, has been discussed in Tenable blog posts⁵. At this time, there are at least four families of malware targeting POS systems⁶; these threats can have significant economic impact on retailers and consumers.

¹ https://discussions.nessus.org/community/indicators-of-compromise-and-malware/blog/2014/03/24/malware-s-journey-from-hobby-to-profit-driven-attacks
² http://en.wikipedia.org/wiki/ILOVEYOU
⁴ http://www.forbes.com/sites/emc/2013/08/14/ransomware-spreads-to-mobile-devices/
⁵ https://discussions.nessus.org/thread/6993
⁶ https://discussions.nessus.org/thread/7040
Espionage-based malware has not been forgotten in the last year. Anti-virus vendors have released detailed analysis of long-running malware with names like Snake⁷, Mask⁸, and RCS Spyware⁹. In some cases, these types of malware have been in place nine years or longer, and judging from certain indicators, were written by state-sponsored parties.

Virtually all anti-virus vendors are reporting a marked increase in malware that targets mobile devices. Several technical news sources were near continuous in 2013 on how the numbers doubled from 2012 to the same time in 2013. This is due to multiple factors, including the high-volume adoption of smart phones, mostly running the same core operating systems, and the way those phones do not have the low-level security software packages that can be leveraged on PCs. While there is security software for the Android platform (which is the most targeted) as well as the iPhone, in neither case is the protection real-time, and is relegated to the task of scanning objects after they are delivered to the mobile device. This limitation is a deliberate effort by mobile device vendors to have all software run in a sandbox to prevent the devices from being compromised by malware.

This strategy of targeted and drive-by low traffic malware has worked well for malware authors. Malware continues to grow with 100,000 new samples being analyzed in malware labs every day. While malware authors are moving towards the less-protected mobile devices, they will still continue to target valuable endpoints and servers. It does not appear that these trends will change any time soon.

**Strategies for Building Effective, Long-Term Malware Defenses**

Malware defense structure can be an intimidating and expensive undertaking. Many times the answers given by vendors and consultants seem to be:

1. “spend more money” and/or
2. “buy my product” and sometimes,
3. “You haven’t implemented it correctly.”

By now, you may have also heard, “Anti-virus is dead.” When it comes to the evolving endpoint-security marketplace, you could easily be wondering who and what to believe.

Rather than insisting that you can only achieve effective malware defense by implementing new gear, there are some different approaches that may be appropriate for your enterprise. Let’s start with a layered-defense concept that was developed in 2002, published in 2003¹⁰, and re-evaluated for and presented at the 2008 Virus Bulletin Conference¹¹. This concept is illustrated in Figure 1 below:

---

⁷ [https://discussions.nessus.org/thread/7178](https://discussions.nessus.org/thread/7178)
⁸ [https://discussions.nessus.org/thread/7087](https://discussions.nessus.org/thread/7087)
⁹ [https://discussions.nessus.org/thread/7100](https://discussions.nessus.org/thread/7100)
Remarkably, the organization in which this was developed still uses the basic framework with a high degree of success. Some of the nuts and bolts may change, like anti-virus product X is replaced by anti-virus product Y, firewall vendor Z is replaced by vendor A, and Android or iPhone users are treated like any other level 1 mobile or remote user. Even with those changes, the base architecture remains the same. By implementing zones, treating each endpoint as an access point as well as an endpoint, and monitoring the devices as well as the network, the organization casts a wide and deep net of defenses that can be implemented in organizations of any size.

This defensive model leverages multiple best-of-breed tools in a mutually supportive architecture. Even with specially crafted targeted attacks and drive-by downloads, malware still needs to communicate with controllers and make modifications to the targeted host. Leveraging the strength of active and passive detection and monitoring provides the best chance for prevention and rapid detection of any penetrations.

**Extending Existing Malware Defenses with Next-Generation Capabilities**

With the increased technicality of the threats, emphasis on the previous architecture needs to shift from one set of tools to another option. While at the time of the initial architecture concept, the primary tools in network defense were endpoint protection and firewalls, these tools are not highly agile and allowed some threats to bypass their defenses. This was acknowledged at the time, so non-traditional defenses were incorporated into the architecture. These were devices such as honeypots and network sniffers, which were called the Virus Monitoring Devices (VMD). With the migration of the threats as we’ve discussed earlier, the more agile VMDs should become the predominant detection devices.

A portion of these VMDs were coined as “worm charmers” and have been discussed in several presentations. These worm charmers took advantage of open-source tools such as honeypots and Snort to detect previously unknown malware on the network. The concept of worm charming merged into the tools many of us know as Intrusion Detection Systems (IDS) and has been incorporated to most network defenses.

---

As previously mentioned, malware needs to communicate and make modifications on compromised hosts. With rare exceptions, both an infection artifact and communications must be present. The artifacts can be registry or file modifications, file creations or other OS manipulation. This is required to keep the machine infected upon reboot. While there is some malware that can do its dirty work in memory, once the machine is shut down or rebooted, it is no longer a threat. Similar malware replicates, receives instructions (in some cases updates), and exfiltrates data via communications. While threats such as the Heartbleed vulnerability don’t leave an artifact, they are very rare but still require communications.

The network defender gains more flexibility by leveraging network sensors and network-based vulnerability scanners in an enhanced manner. Since these tools are not looking for specific threats or malware (unless directed to), they report a lot of information. When the defender knows what is normal on their network, abnormal traffic becomes an item of interest and an indicator of potentially malicious activity. These tools can also be used to monitor for specific activities that have been reported to be hostile or suspicious.

These monitoring tools can also be used in a forensics and response mode. Monitoring the communications of a known compromised host helps identify other compromised hosts or command and control modules. Organizations have used this method to uncover hostile tactics and techniques to identify attackers to pursue legal action, as well as identify previously unknown holes in their network defense.

**Conclusion and Next Steps**

While the malware threat is not going away and is being driven by financial interests, the threat is not overwhelming. Organizations will continue to suffer targeted attacks, be it for espionage or theft. The best defenses against these attacks continue to be a well-designed, integrated, and flexible defense in depth.

Enhancing existing defenses does not necessarily mean spending more money. Most organizations already deploy network sniffers, vulnerability scanners, and intrusion prevention and detection scanners in addition to the traditional counter-malware and endpoint security products. By combining the resources already at their disposal and centralizing reporting, a security team will find many of their tools are useful in ways they did not initially envision.

Keys to this strategy are coordination, knowledgeable system management, and flexible reporting. It’s easy to lose sight of the network architecture by not knowing what is deployed or what vulnerabilities or other activities are occurring on your network. Once a baseline is identified, abnormal activity becomes an indicator and can be investigated or otherwise properly handled. At the same time, traditional means of endpoint protection are leveraged for their strengths: identifying and preventing known attacks or threats.

There is no such thing as a perfect defense. This is true in the digital world as much as it is in the physical. Proven tools such as endpoint protection, firewalls, and network monitors provide a solid foundation for defense. When leveraged properly allowing each tool to do the job it was designed for, a high level of protection is possible. Coupling in user education and a proper response plan will further minimize exposure and risk.

When it comes to delivering enhanced Virus Monitoring Device (VMD) functionality for your enterprise, the combination of Tenable’s Nessus® active vulnerability scanner, Passive Vulnerability Scanner™ (PVS), Log Correlation Engine (LCE), and SecurityCenter™ – delivered as Tenable SecurityCenter Continuous View (SC CV) – provides capabilities far beyond any point solution. SC CV correlates detected malware data with vulnerability scan data. It provides reports, dashboards, and alerts that help you quickly identify and mitigate the most critical and imminent threats. By deploying SC CV in your environment, you can:

- Directly detect the presence of malicious processes on physical, virtual, and mobile devices
- Identify devices on your network communicating with known botnets and CnC servers
- Discover configuration files that may have been tampered with by malware
- Monitor registry settings for signs of compromise
- Audit AV and other security tools to ensure they are up to date and operational

Visit [http://www.tenable.com](http://www.tenable.com) to learn more about Tenable’s continuous monitoring solutions for the new IT landscape.
About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world’s largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard to identify vulnerabilities, prevent attacks and comply with a multitude of regulatory requirements. For more information, please visit www.tenable.com.