Threat vectors – what are they and why do you need to know them?

Topics: Advanced Threat Protection, Attacks and Threat Actors, Reader Favorites, Series: Understanding ransomware, State and Local Government

November 17, 2016 | Slawek Ligier

Note: This is part 2 in our Ransomware series by Slawek Ligier

In our last post, we introduced this series and discussed the concept of ransomware. This time we'll talk about threat vectors and why you should be thinking in terms of threat vectors rather than specific attacks.

Put simply, threat vectors are the routes that malicious attacks may take to get past your defenses and infect your network. We will be talking about six threat vectors in particular:

- Network – The perimeter of your network, usually protected by something like a firewall.
- User – Attackers often use social engineering and social networking to gather information and trick users into opening a pathway for an attack into a network.
- Email – Phishing attacks and malicious attachments target the email threat vector.
- Web Application – SQL Injection and Cross-Site Scripting are just two of the many attacks that take advantage of an inadequately protected Web Application threat vector.
- Remote Access – A corporate device using an unsecured wireless hotspot can be compromised and passed on to the corporate network.
- Mobile – Smart phones, tablets, and other mobile devices can be used as devices to pass malware and other attacks on to the corporate network. Additionally, mobile malware may be used to steal use data from the mobile device.

Devising a strategy around threat vectors offers the depth and breadth necessary to achieve what Barracuda refers to as Total Threat Protection. This is a comprehensive framework that integrates best-of-breed security components and real-time protection. This short video goes into some detail on this:

We also have more information on threat vectors and Barracuda Total Threat Protection in this Google Hangout.

In addition to threat vectors, you also have to consider your attack surfaces. The vulnerabilities and exposed resources of a threat vector represent an attack surface. For example, consider the scenario used in this SANS Technology Institute article:

- We are spending more money to develop an increasing number of web applications that are often mission critical.
- At the same time attackers are getting better at exploitation of web applications.
- At the same time companies like Ameritrade and TJX have suffered massive data breaches leading to class action lawsuits and potentially, another wave of government regulations+

So we can see that software attack surface, especially web application software, is a significant problem.

Here are the steps to take to minimize the attack surface in the web application threat vector:

- Reduce the amount of code executing, turn off features

- Reduce the volume of code that is accessible to users, a form of least privilege
- Limit the damage if the code is exploited[5]

As you can see, there may be multiple vulnerabilities in a single threat vector. The complete sum of these vulnerabilities is the attack surface.

In order to fully assess your risk, you have to be able to identify your threat vectors and the attack surfaces within them. To secure these threat vectors, think in terms of multiple layers of protection (depth) and integrated best-of-breed solutions that work together seamlessly (breadth).

Click here for the OWASP Attack Surface Analysis Cheat Sheet

Ransomware and other attacks use multiple threat vectors to gain entry to your network. For example, a spam / phishing campaign could include a compromised attachment. A visit to a corporate website could result in a malicious download, if that website had been attacked. A popular piece of software could be infected and purposely downloaded by the user. This is what happened with Linux Mint earlier this year. As you can see, the same threat can hit more than one threat vector.

This should give you a good idea of how threat vectors work, and why it is so important that you understand them.

For more information on ransomware, visit these resources:

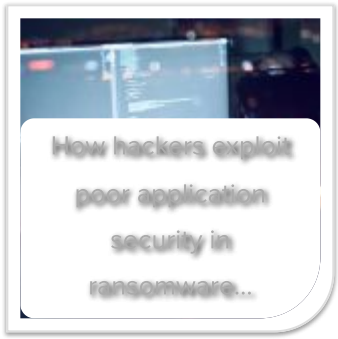
- NoMoreRansom project
- The evolution of ransomware
- Microsoft Malware Protection Center
- Ransomware blog posts

To view all posts in the series, click here.

Next time we'll talk about Deep Machine Learning, Advanced Threat Detection, and other protection technologies.

Slawek Ligier

Related Posts:



Previous blog post

Next blog post

Subscribe to this blog

Please enter your email

SUBSCRIBE

Subscribe to this blog

Email

SUBSCRIBE

Search

Popular Posts

Atlassian Confluence RCE vulnerability: CVE-2022-26134

Ransomware offensive gets underway

Cybersecurity Threat Advisory: Microsoft Windows critical remote code execution vulnerability

Barracuda celebrates partner success at Discover'22

Threat Spotlight: Attempts to exploit new VMware vulnerabilities

Topics

13 Email Threat Types

Public Cloud Security

Remote Work

Email Protection

Network Security

Application Security

Data Protection and Recovery

Barracuda Engineering

Managed Services

Training and Awareness

Office 365

SD-WAN

K-12 Education

Internet of Things (IoT)

Life@Cuda

Resources

Barracuda Security Insights

Barracuda Email Threat Scan

Security Glossary