# Looking Deeper into a Multi Stage Attack

by admin | Dec 12, 2016 | Blog |

The majority of today's breaches are comprised of sophisticated multi-stage attacks. The stages of such attacks can best be described by a "Cyber Kill Chain", which breaks down cyber intrusions into the following steps: Recon → Weaponize → Deliver → Exploit → Install → Command & Control → Action. Most inline or endpoint protection products have the capability to detect one of the stages of an attack, but lack the ability to analyze the entire activity chain. This prevents security operations teams from seeing the full context of the attack. If one were to allow the attack to be played out completely, one can learn more about these threat actors, making it easier to stop future attacks.

In this blog, I will demonstrate this using a case study of a common attack. This particular attack was stopped by a perimeter based device. Based upon the analysis of the attack, we will discuss internal security weaknesses in organizations. I will then discuss one of the recommended approach for analyzing a multi-stage attack that is aimed at identification and remediation of the internal weak links in an organization.

Search

## Recent Posts

The New York Post – This Teen Made $100,000 For Legally Hacking Major Companies

MarketWatch – This 18-Year-Old's Hacking Side Hustle Has Earned Him $100,000 — And It's Legal

BrightTALK – TAG-Cyber's Ed Amoroso Interviews Acalvio

3 Minutes Until the Apocalypse –

Figure 1 shows a file titled “Verify.pdf”, which was stopped by an email filtering solution. Since there is a mismatch between the comment, which shows as Bank of America, and the email address, which shows as kolumbus.fi, the file is declared as malicious and is quarantined.

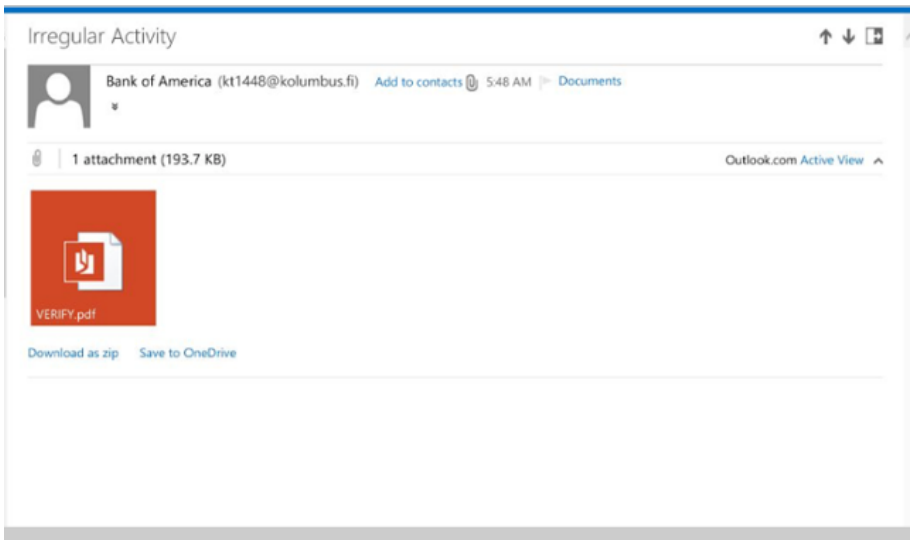


**Figure 1 – Malicious attachment detected by Email Filtering Solutions.**

When the attached PDF file is dissected, as shown in figure 2, it can be seen that the file is a making an HTTP request:


**Figure 2.0. HTTP request inside the PDF**

If we do a quick search for the domain, as shown in figure 3, it is malicious and is detected by one vendor Trustwave.

Technical White Paper

TAG Cyber Interview of Acalvio’s John Bradshaw

## Archives

July 2018

June 2018

May 2018

April 2018

March 2018

February 2018

January 2018

December 2017

November 2017

October 2017

September 2017

August 2017

July 2017

June 2017

May 2017

April 2017

March 2017

February 2017

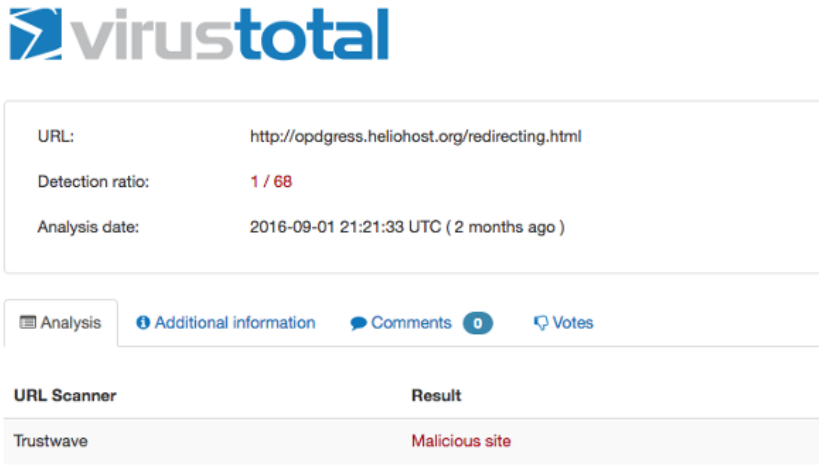


**Figure 3 – Virustotal Detection of the Embedded URL link**

However, if we check for the endpoint detection of the pdf file, as per VirusTotal figure 4, it evades 53 endpoint protection products.


**Figure 4.0 Virus Total Score for the File**

Based upon this quick analysis of the stopped threat, it can be observed that even though the threat got stopped, there are many internal weak links in an organization:

- Detection of the malicious pdf downloader (as shown in figure 4.0 ) at the end point is missing. If the malicious pdf downloader would have been able to reach the end point via some other delivery mechanism it would have infected the organization.
- Detection of the malicious communication (as shown figure 3.0 ) by the network inspection devices is almost non-existent, since true targeted attacks will contain a fresh, previously unknown C&C server that is not in any known blacklist.

January 2017
December 2016
November 2016
October 2016
September 2016
August 2016
July 2016

## Categories

Analyst Reports
Blog
Data Sheets
E-Books
Events
In the News
Press Releases
Resources
T-Shirts
Video
Webinars
White Papers

- One of key indicators to detect the threat is a mismatch of comment in the email address, which is "Bank of America" and email address "kt1448@kolumbus.fi". If the descriptor (Bank of America) was missing, then the same attack might have been able to reach the endpoint via email. So the detection algorithm to stop the attack can be bypassed by a variation of the attack.

These weak links can be exploited by other threat actors attack who leverage slight variants of it.

Given that majority of breaches these days involve multi stage attacks, the recommended architecture for the analysis of the multi stage threat, will be to have a threat analysis platform which allows execution and analysis of every stage of a threat. In order to determine if an entity is malicious, besides using analysis algorithms, Threat Analysis platform must also leverage time-independent correlations, which gives an ability to correlate the events which happened before or after in a virtualized network, to classify an entity as malicious. In this way, each malicious entity which was part of the threat gets detected. Identification of every malicious entity of the threat will allow an organization to capture all the malicious indicators involved in a multi stage attacks, and not just the initial stages. This can then can be used to strengthen internal defenses in a more robust and comprehensive manner.

of deployment, monitoring and management. Acalvio enriches its threat intelligence by data obtained from internal and partner ecosystems, enabling customers to benefit from defense in depth, reduce false positives, and derive actionable intelligence for remediation.