Detection of Prevalent Threats by Distributed Deception

by Abhishek Singh | Apr 2, 2018 | Blog |

Today's breaches are overwhelmingly carried out in a series of sophisticated, multi-stage attacks. The stages of such attacks can best be described by a "Cyber Kill Chain," which as per MITRE ATT&CK Adversary Tactic Model [1] breaks down cyber intrusions into the steps shown in figure 1.0.

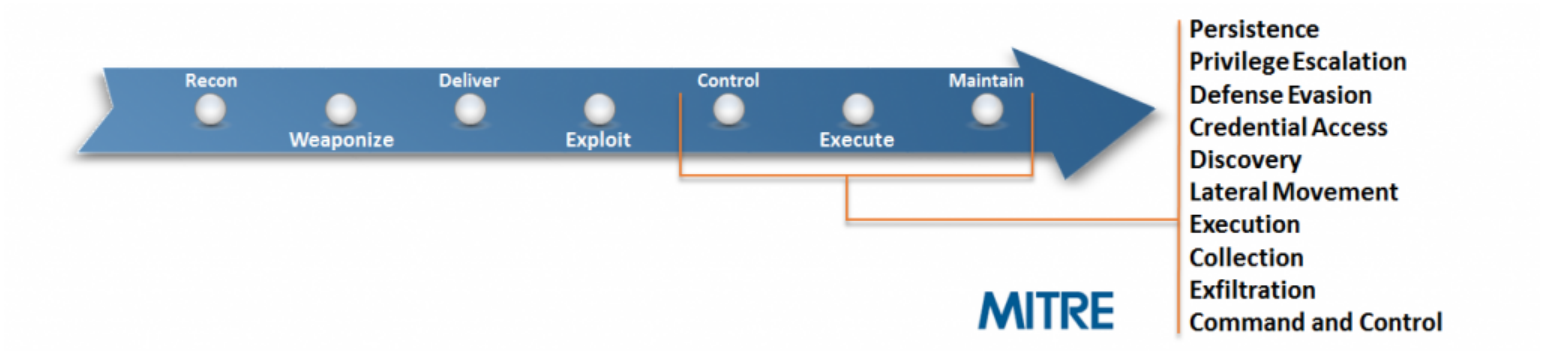

Figure 1.0 MITRE ATT&CK Adversary Tactic Model

In the table 1.0, I have discussed six critical multi-stage attacks. I have precisely listed the breadcrumbs and lures that are required at the endpoint and deceptions on the network to detect and divert these threats. The table further lists the conditions which when triggered will raise the alarm for breach and the stage where the threat will get discovered. This stage is as per the ATT&CK Matrix for Enterprise[1]. Based on the nature of the threat, once an alert for a breach is raised it can trigger appropriate automated responses. Examples of responses include: isolation of the infected

endpoint, SOC Alert for remediation, etc.

The six threat families considered in this blog are::

1. Ransomware[5]
2. Crypto Miner[2]
3. Breaches leveraging Web Servers for entry [4]
4. Destructive malware (such as Shamoon[3] and Petya[6])
5. Information stealers
6. Password stealers

In our blogs listed in references, we have discussed the exploitation steps of these threats. These threats also have been covered extensively within the research community.

Threat Class	Malware in the Threat Class	Detection Stage as per Mitre Threat Matrix	Condition leading to the detection of breach	Breadcrumbs /Lures on the endpoint	Deception on the internal network
Destructive Malware	Shamoon, Olympic Destroyer, Petya	Lateral Movement	Brute force attempt, detection of RCE, usage of honey credentials to log on to SMB deceptions, SMB exploit class packets	Entry of deceptions such as SMB, DB, in the ARP table, Established connection to deceptions in network. Honey credentials in lsass.exe.	Projected SMB deceptions in the subnet
Ransomware	99% of the Families	Execution Phase	Encryption of Honey files will trigger proprietary algorithm.	Honey Files, Mapped Drives	Honey Unmapped Drives.
Cryptominer	WannaMine, Zealot campaign, ReddisWannaMine	Lateral Movement Phase	Network scanning, detection of RCE, usage of compromised credentials., SMB exploit class packets	Established connection from every network adaptor of Web Server, Endpoint to SMB, DB, FTP deceptions. Honey credentials in lsass.exe	Deceptions such as SMB, DB, FTP in the subnet. Deceptions having Class B IPv4 address.
Information Stealer	Emotet, Qakbot	Lateral Movement Phase	Brute force attempts, usage of compromised credentials.	Honey username and deception services in AD. Honey credential on the endpoint. Honey email address in Outlook	Projected SMB deceptions in the subnet
Breaches involving Web Server	Remote code Apache Struts e.g. CVE-2017-5639, CVE-2017-9822, WebShells	Lateral Movement Phase	Detection of Scan originating from Web Server, detection of RCE, usage of honey credentials to log on to deceptions, brute force attempts, SMB exploit class packets	Established connection from Webserver to Deceptions. Honey Password in lsass.exe	DB, SMB, FTP deception reachable from Webserver, Deceptions having class B IPv4 addresses.
Password Stealer	Pony password stealer, Ovidiy password stealer	Execution Phase	Usage of compromised password to log on to honey services such as SQL, FTP, SMB	Honey credentials in the browser, Registry Entries and at specific locations	Deceptions such as SMB, DB, FTP in the network.

Table 1.0 Showing the detection of Critical Threats using Distributed Deception.

By using a distributed deception platform, two of these threat families (ransomware and password stealers) is detected in the execution phase. The other four are identified during the lateral movement phase when the attacker is attempting to spread to other machines.

Based on the analysis shown in the table following is the takeaway:

- Deception centric architecture detects the second or subsequent stage of payload,

and hence the detection of distributed detection becomes independent of the vulnerability which is exploited at the first stage. The first stage can make use of 0-days, or it can make use of the known vulnerability or even socially engineer humans into giving them access via phishing or socially-engineered malware, a deception-centric architecture will raise an alert if the second or subsequent phase touches the deceptions.

- In many of the cases such as breaches involving web server, detection of information stealer, detection of crypto miners, detection of destructive malware presented in the table above, distributed deception architecture is capable of detecting threat actor or worm after it has breached an organization before the final intent is completed. The algorithm or the techniques leveraging deception which is used to identify the threat is generic, i.e., it is independent of the purpose of the worm or the threat actor.

The capability of detecting worm or an adversary independent of the first stage and detecting a breach in a generic manner independent of the final intent makes it a recommended architecture to prevent sophisticated breaches.

References

[1] ATT&CK Matrix for Enterprise, https://attack.mitre.org/wiki/Main_Page

[2] WannMine lateral Movement techniques,

https://www.acalvio.com/wannmine-lateral-movement-techniques/

[3] How to outfox Shamoon, put deception to work,

https://www.acalvio.com/wannmine-lateral-movement-techniques/

[4] Deception Centric Architecture to prevent breaches involving Web Server,

https://blog.acalvio.com/deception-centric-architecture-to-prevent-breaches-involving-webserver/

[5] Deception centric defense against the Ransomware

. .https://www.acalvio.com/deception-centric-defense-against-ransomware/

Recent Posts

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 – Technical White Paper

TAG Cyber Interview of Acalvio's John Bradshaw

Security Week – Outdated DoD IT Jeopardizes National Security: Report

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

January 2017

December 2016

November 2016

October 2016

Categories

Acalvio provides Advanced Threat Defense (ATD) solutions to detect, engage and respond to malicious activity inside the perimeter. The solutions are anchored on patented innovations in Deception and Data Science. This enables a DevOps approach to ATD, enabling ease 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.