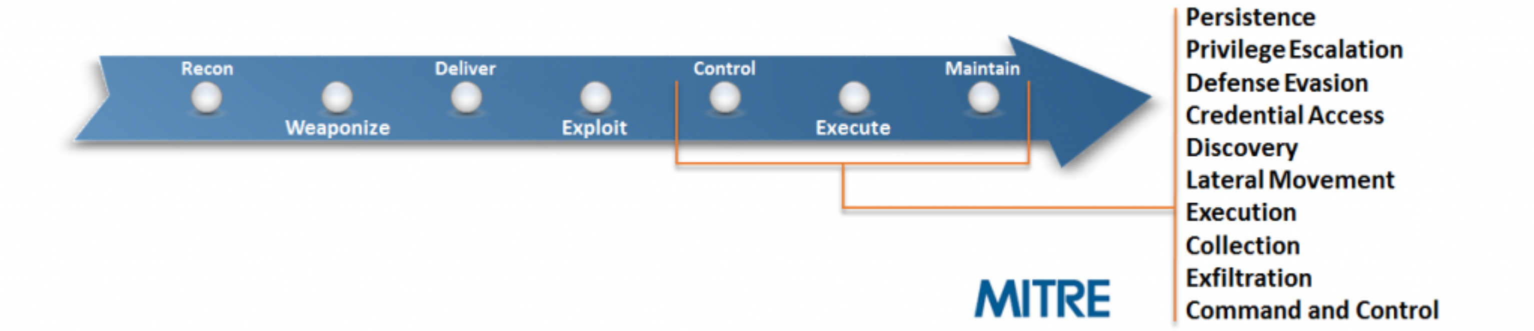
Detection of Breach Campaigns by using Distributed Deception

by Abhishek Singh | May 17, 2018 | Blog |

Today's breaches are predominantly carried out in a series of sophisticated, multi-stage attacks. The stages involved in such an attack can best be described by a "Cyber Kill Chain". This, as per MITRE ATT&CK Adversary Tactic Model [11] breaks down cyber intrusions into the steps shown in the following figure.



As discussed in the previous blogs and the white paper deception solution deploys breadcrumbs and lures at the endpoint. These breadcrumbs and lures can be :

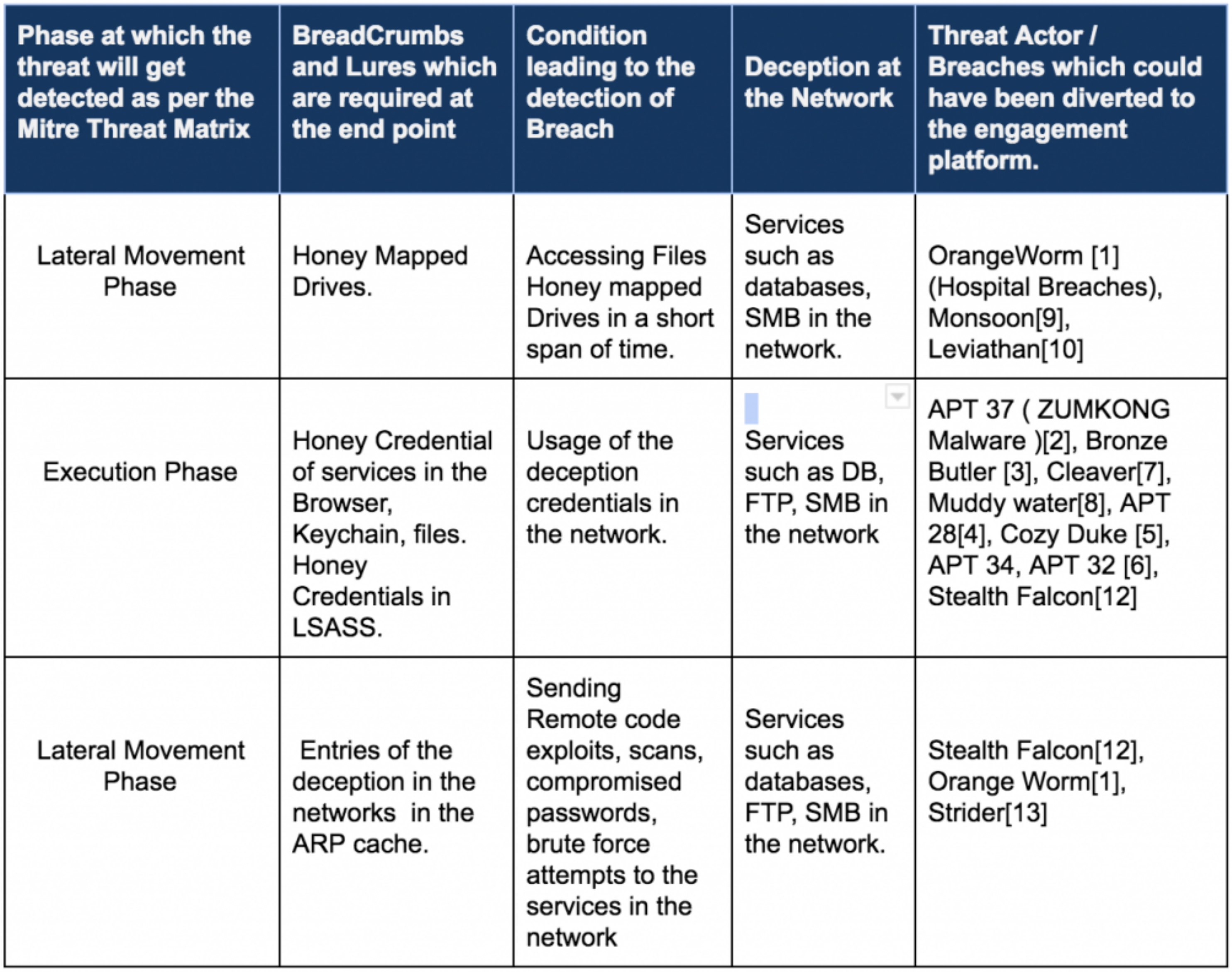
- Honey authentication values in the browsers such as adding honey authentication in "HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\IntelliForms\Storage2" for IE7, honey authentication values at "\Local\Google\Chrome\User Data\Default\Login Data" for Chrome etc..
- Honey mapped drives
- Honey entries in the ARP cache

- Honey RDP links,
- Honey entries in the keychain
- Honey entries in the files such as password files under %APPDATA% folder.
- Honey entries in the active directory
- Honey connection from the Endpoint / Web Server to the services such as databases in the network,
- Honey email addresses in the address book of Outlook,
- Honey DNS server,
- Honey authentication values in the processes such as lsass.

These end-point lures point to the honey services such as SMB, FTP, Databases in the subnet. Since the static breadcrumbs are interspersed with the real endpoint assets, there is always a possibility of legitimate assets getting used by a threat actor. This problem of legitimate assets getting used by the threat actor can be reduced by increasing the density of the breadcrumbs and lures at the endpoint.

If there are "m" legitimate services and "n" honey services then if { [m / (n + m)] <= 0.001} it will ensure the probability of accessing legitimate services remains less than equal to 0.1 %.

In our previous blog, we analyzed six prevalent worms and malware. We discussed the precise breadcrumbs and lures that are required at the endpoint and honey services in the network and the conditions that will lead to their detection. In the following table 1.0, we have taken three breadcrumbs and listed the breaches that could have been diverted by using these breadcrumbs. The three breadcrumbs which we have considered are honey entries in the ARP cache, honey mapped drives and honey passwords in the browser and in the processes such as lsass. The reports of these breaches have been published publicly and are mentioned in the references.



Phase at which the threat will get detected as per the Mitre Threat Matrix	BreadCrumbs and Lures which are required at the end point	Condition leading to the detection of Breach	Deception at the Network	Threat Actor / Breaches which could have been diverted to the engagement platform.
Lateral Movement Phase	Honey Mapped Drives.	Accessing Files Honey mapped Drives in a short span of time.	Services such as databases, SMB in the network.	OrangeWorm [1] (Hospital Breaches), Monsoon[9], Leviathan[10]
Execution Phase	Honey Credential of services in the Browser, Keychain, files. Honey Credentials in LSASS.	Usage of the deception credentials in the network.	Services such as DB, FTP, SMB in the network	APT 37 (ZUMKONG Malware)[2], Bronze Butler [3], Cleaver[7], Muddy water[8], APT 28[4], Cozy Duke [5], APT 34, APT 32 [6], Stealth Falcon[12]
Lateral Movement Phase	Entries of the deception in the networks in the ARP cache.	Sending Remote code exploits, scans, compromised passwords, brute force attempts to the services in the network	Services such as databases, FTP, SMB in the network.	Stealth Falcon[12], Orange Worm[1], Strider[13]

Table 1. 0 Showing the diversion of breaches by using breadcrumbs at the endpoint.

From the above table we can draw the following inferences:

- The deception platform gets triggered during the Credential Access, Discovery, Lateral Movement phases. Hence it complements other defenses which get triggered during the Initial Access, Execution, Persistence, Privilege Escalation, Defensive Evasion phases. These phases are as per the MITRE ATT&CK Matrix for the Enterprise.
- In some of the breaches, for example, Orangeworm [1] reported on April 23rd, 2018, targeting hospitals, a deception platform would have been able to divert the multi-stage attack at multiple places by having honey entries in the ARP cache and also by having honey drives.

These inferences make deception based architecture a recommended architecture to prevent modern-day breaches.

References:

[1] New Orangeworm attack group targets the healthcare sector in the U.S. , Europ, and Asia https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-

healthcare-us-europe-asia

[2] APT 37 The overlooked North Korean Actor, https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

[3] Bronze Butler Targets Japenese Enterproses https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

[4] A window into Russian Cyber Espionage Operations ? https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

[5]Cozy Duke, https://www.f-secure.com/documents/996508/1030745/CozyDuke

[7]Operation Cleaver, https://www.cylance.com/content/dam/cylance/pdfs/reports/Cylance_Operation_Cleaver_Report.pdf

[8] Muddying The Water : Targeted Attacks in The Middle East https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

[9] Monsooon Campaign https://github.com/Cyb3rWard0g/ThreatHunter-Playbook/blob/master/adversary_attribution/MONSOON.md

[10] Leviathan https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

[11] Mitre ATT&CK Adversary Model, https://attack.mitre.org/wiki/Main_Page

[12] Stealth Falcon, https://citizenlab.ca/2016/05/stealth-falcon/

[13] Strider, https://github.com/Cyb3rWard0g/ThreatHunter-Playbook/blob/master/adversary_attribution/Strider.md

Search

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

September 2016

August 2016

July 2016

Categories

Analyst Reports

Blog

Data Sheets

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.