Translating Deception into a Technology which can Detect Current day Breaches and Threats.

Abhishek Singh

Translating Deception into a technology which can detect threats

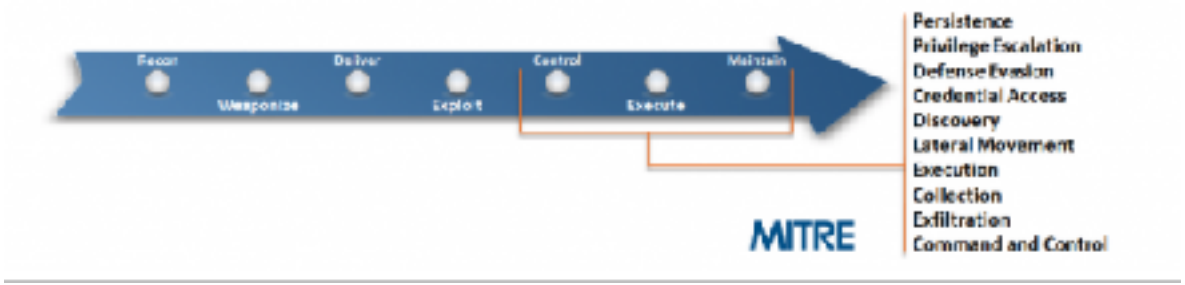
Two main questions

- Why one more detection technology ?

- What is the challenging ?

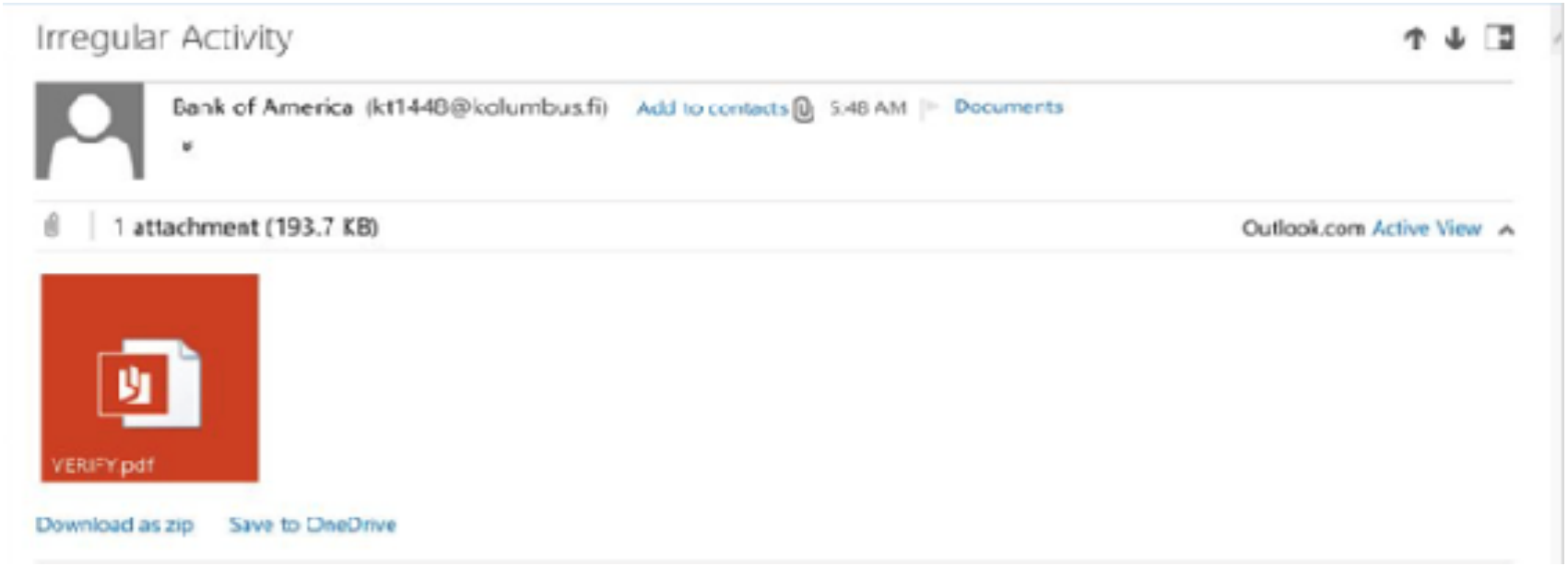
Why one more detection technology ?

- Modern day attack and breaches are multistage attack which can be broken into



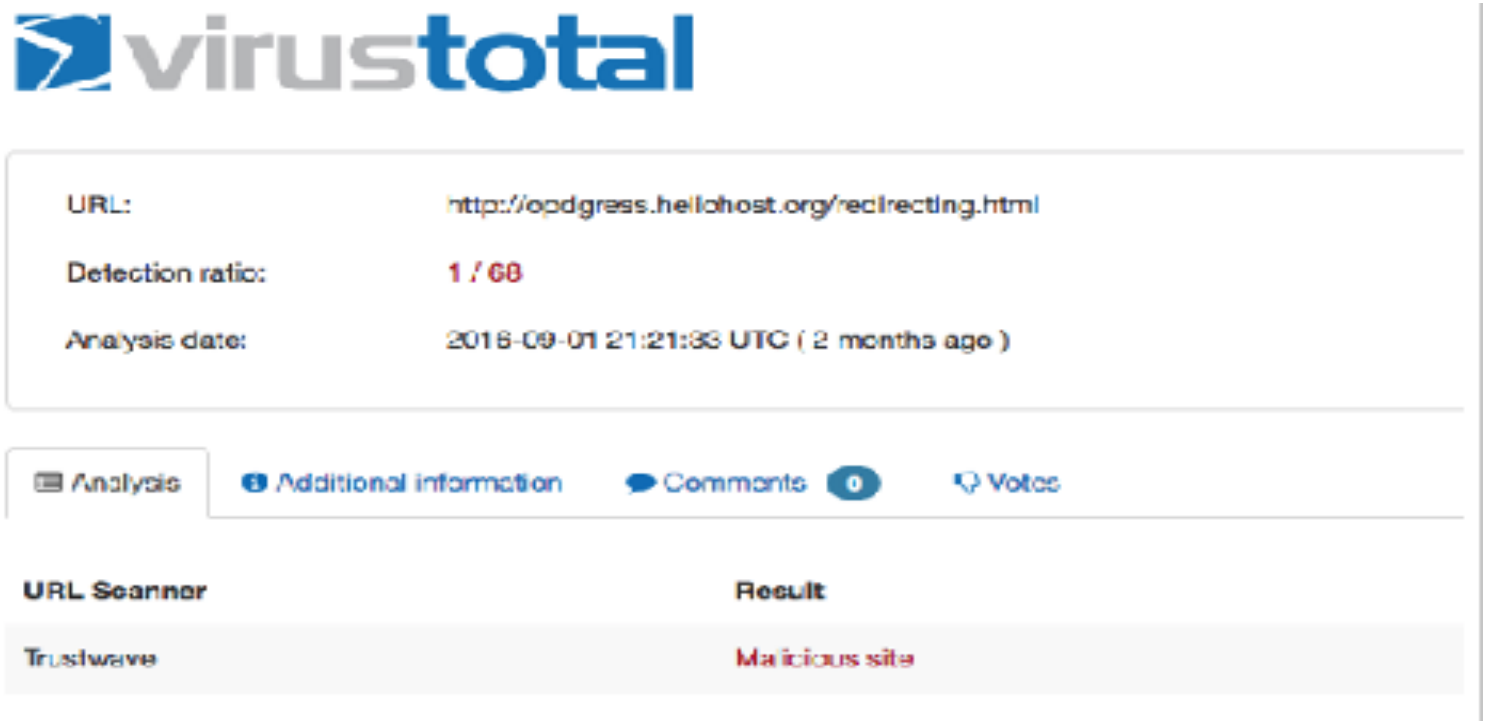
- Detecting one stage necessarily does not mean we know details of every other stages.

Explain it with an Example. Attack was stopped.



Dissecting PDF. It has link to download a file

Link gets detected by one AV



PDF is undetected by 53 Endpoint AV.

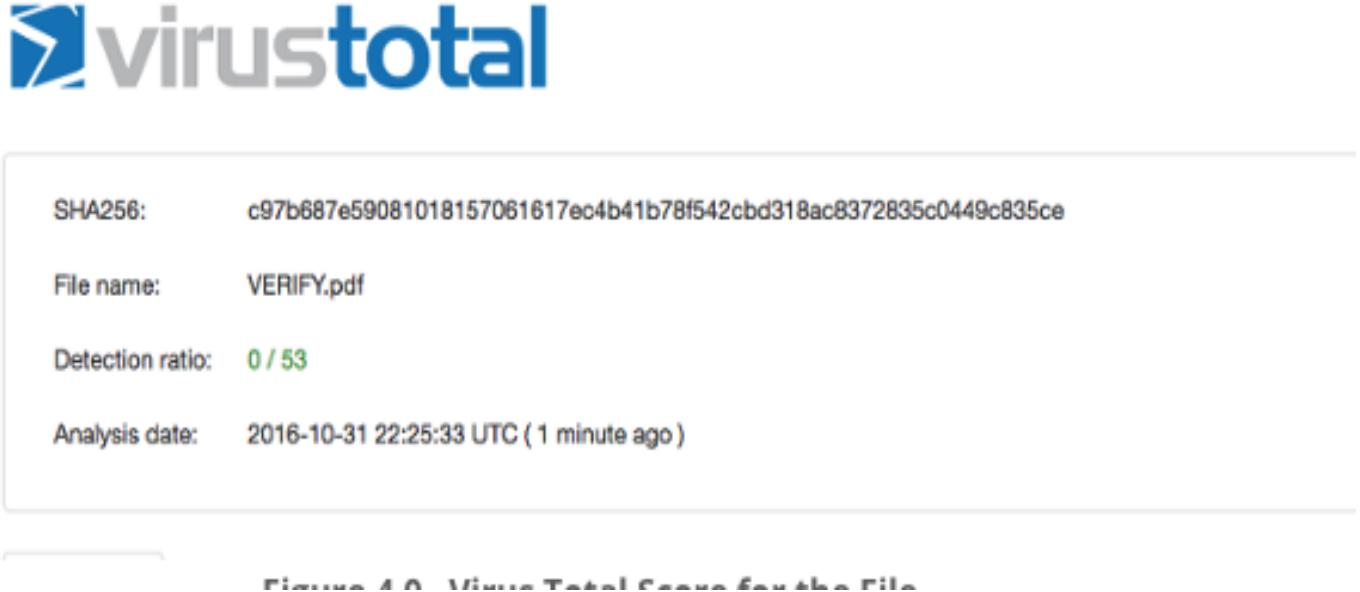


Figure 4.9 - Virus Total Score for the File

Let’s Summarize the attack

- Detection of the malicious pdf downloader 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 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.

Let’s Summarize the attack

- 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.

Why one more detection technology ?

To counter the current day threats and breaches such as

- Swift Hack at Bangladesh Bank
- Equifax Breach. …...

Detection technology should be able to detect the attack, divert the attack and all allow all the steps to execute. Once all the steps have been executed, analyze each steps to identify every hidden IoC which then can be used to harden internal systems.

This is where deception based technology can be used. How is explained in later slides.

Why it is Challenging ?

- First form of deception. Place fake services (Honeypots) in the network and threat actor will trip over it. This will not work.

Using first form of deception to detect sophisticated day breaches == Horse Carriage to win Formula One Race.

Before coming up with appropriate architecture it is important to take a step back and understand the lateral movement techniques employed by worms and threat actor.

Ransomware : Mapped Drives for Lateral Movement.

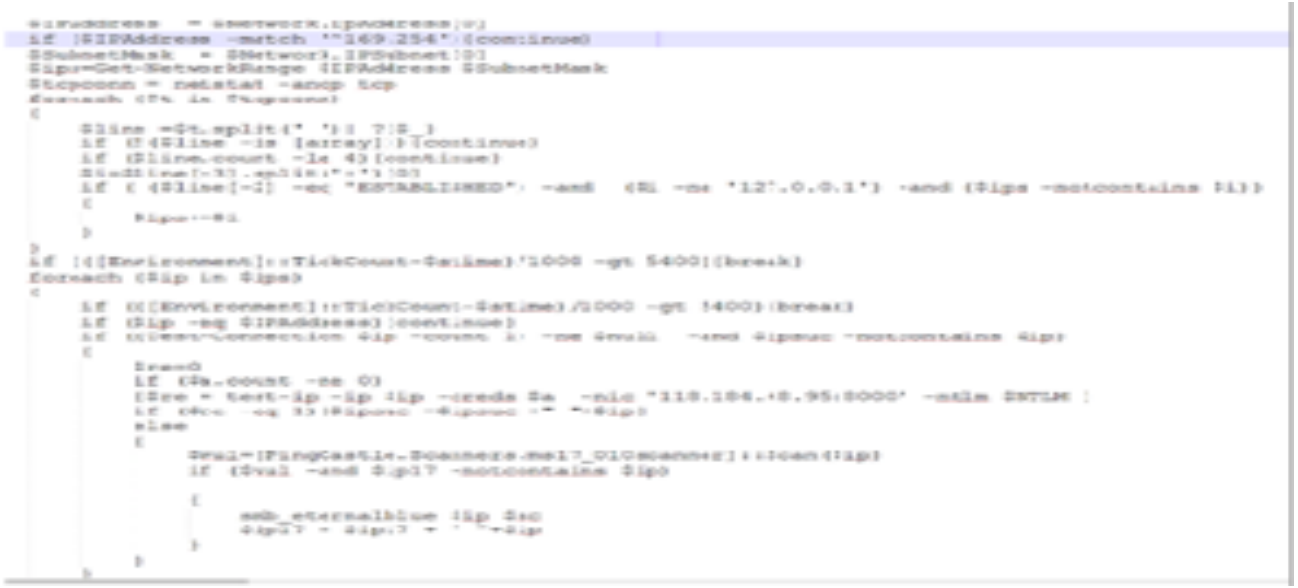
```
u8 = GetLogicalDrives();
v1 = 2;
v2 = 2;
do
{
  result = 1 << v2;
  if ( (1 << v2) & u8 )
  {
    RootPathName = (unsigned __int8)v1 + 97;
    u5 = 58;
    u6 = 92;
    v7 = 0;
    result = GetDriveTypeW(&RootPathName);
    if ( result == 3 || result == 2 || result == 6 )
    {
      u6 = 0;
      result = sub_402CF0((void *)&RootPathName);
    }
  }
  ++v1;
  ++v2;
}
while ( (unsigned __int8)v1 < 0x19u );
return result;
```

Ransomware : Unmapped Drives for lateral movement.

```
DWORD __cdecl sub_407919(int a1, LPNETRESOURCEW lpNetResource)
{
  DWORD result; // eax@1
  struct _NETRESOURCEW NetResource; // [sp+4h] [bp-80Ch]@3
  DWORD BufferSize; // [sp+808h] [bp-8h]@3
  HANDLE hEnum; // [sp+800h] [bp-8h]@1
  DWORD cCount; // [sp+804h] [bp-4h]@3

  result = WNetOpenEnumW(2u, 1u, 0x13u, lpNetResource, &hEnum);
  if ( !result )
  {
    while ( 1 )
    {
      cCount = 1;
      BufferSize = 2048;
      if ( WNetEnumResourceW(hEnum, &cCount, &NetResource, &BufferSize) )
        break;
      if ( !(NetResource.dwUsage & 1) || !WNetAddConnection2W(&NetResource, 0, 0, 0) )
      {
        if ( NetResource.dwUsage & 2 )
        {
          sub_407919(a1, &NetResource);
        }
        else
        {
          if ( NetResource.dwType == 1 )
            ((void (__cdecl *)(_DWORD))a1)(NetResource.lpRemoteName);
        }
      }
    }
    result = WNetCloseEnum(hEnum);
  }
  return result;
}
```

Crypto Miner Lateral movement : Check for Active Connections.



Lateral Movement Techniques

- Authentication values in the browsers “HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2” for IE7, honey authentication values at “\Local\Google\Chrome\User Data\Default\Login Data” for Chrome etc..
- Mapped drives
- Entries in the ARP cache
- RDP links

Lateral Movement Techniques.

- Entries in the keychain
- Entries in the files such as password files under %APPDATA% folder.
- Entries in the active directory
- Active connection from the Endpoint / Web Server to the services such as databases in the network,
- Email addresses in the address book of Outlook,
- DNS server,
- Scraping the processes such as lsass.

The Execution Steps

- Insert Honey Values (Referred to as Breadcrumbs or Lures) at the end point honey mapped drives, Honey username password in Lsass.exe, Honey Files, honey RDP links, honey email addresses, honey username and password in the browser cache, honey entries in the keychain etc.
- These honey entries will point to the deceptions such as fake services in the network such as SMB, RDP.
- When these fake services are accessed, threat actor will be diverted to the high engagement platform where in attack is allowed to execute , apply heuristic, ML, Behavioral algorithms to gather all the indicators of compromises.
- Once the IoC are being generated, these will act as input to inline IDS, IPS, endpoint, FireWall or can be used for harderning the network,

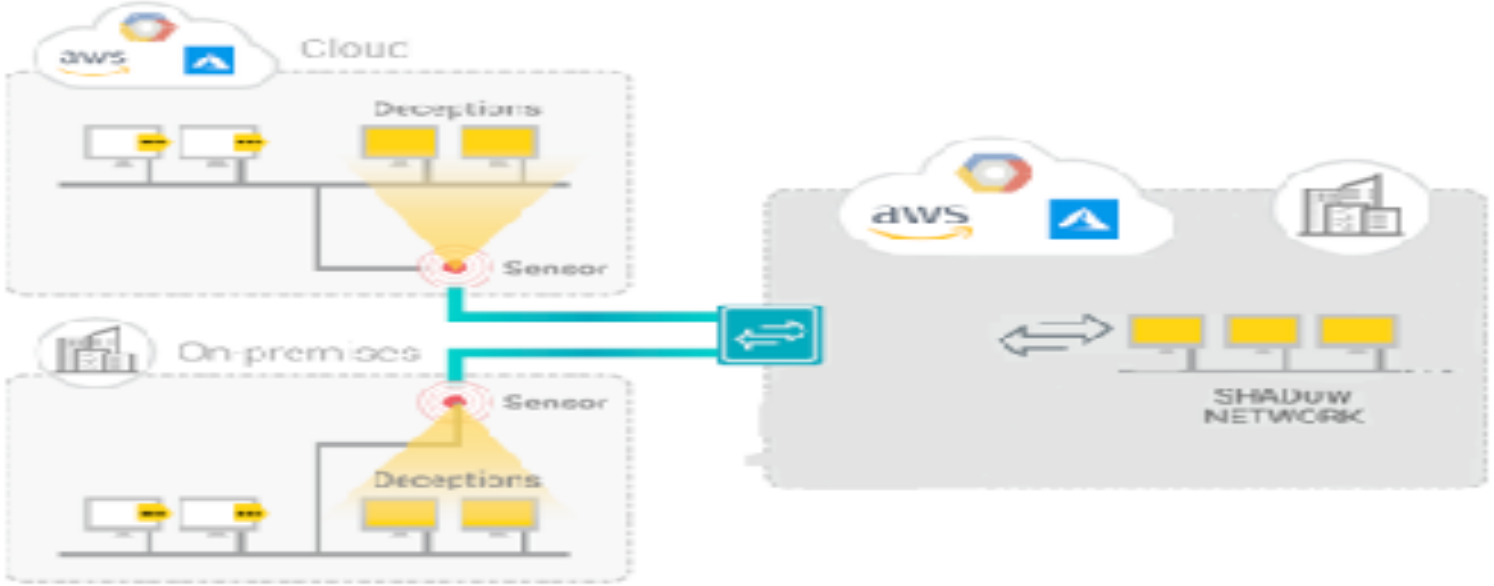
Two Models to add BreadCrumbs at the Endpoint.

- **Static BreadCrumbs:** Advantage Agent less, requires density.

  *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 %.*

- **Dynamic BreadCrumbs** : Through Binary Instrumentation monitor the process and provide the honey values when a process is classified as malicious such as fake email address to AddressEntry.Address, email.search() when a process has been classified as malicious.

Recommended Architecture which Translated to product.



Case Studies to Detect Worms. Ransomware

Behavior of Ransomware

- Encryption of Ransomware: Three Ways.

    -- Open the file, encrypt the content and write to the same file.

-- Moves the file out of directory to temp folder, opens file, encrypts the file & replace the file.

-- Reads a file, creates encrypted file and deletes the files.

Other Behavior of Ransomware.

- Extensions which gets encrypted PDF, Word, PPT, text files at the endpoint, extensions which do not get encrypted EXE, dll, msi, com, bat, xml, BMP, HTML.
- Folders can get skipped \Temp, \Desktop, \Program, \Games, \Samples pictures, \Sample Music.
- Folder always get encrypted C:\users\Public\Documents, C:\users\{users_name}\Documents,
- Deletes Shadow backup “ vssadmin.exe Delete Shadows /All /Quiet “

Detection Algorithm Stateful Model

State 1: Monitor the honey files:

If there is "***write***" operation on honey file or new file "***create***" operation, followed by file "***delete***" operation on honey file, move to state 2

State 2: Compute the Shannon Entropy of the altered file. If greater than 7.9 then the file is encrypted. Move to state 3.

State 3: Check if Honey Shadow Backup is deleted if yes

Suspend the Thread, Raise an alert for Ransomware & Disengage Endpoint (Disabling the Network Adaptor)

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, RedisWannaMine	Lateral Movement Phase	Network scanning, detection of RCE, usage of compromised credentials., SMB exploit class packets	Established connection from every network acaptor 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-2017-5638, 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.

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). Monsoor[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]

Accomplishments

- Ransomware solution was named Hot new Security Product in Black Hat 2017 detecting efficacy of 99.8% .

- Our report "***Spreading Techniques & Deception Based Detection***" was selected nominee for Prestigious Peter Szor 2018 Virus Bulletin Award.

  https://github.com/abhisheksingh1234/Security-Research-/blob/master/Endpoint/Research%20Deception/Spreading-Techniques-and-Deception-based-Detection-Acalvio-Technical-White-Paper.pdf

Q & A