AFRICAHACKON

An Anatomy of a Targeted Attack

Who

Gabriel Mathenge

- Security enthusiast.
- Red teaming and penetration testing.

- **Twitter:** @_theVIVI
- **Website:** thevivi.net
- **Email:** gabriel<at>thevivi.net

Vince Obilo

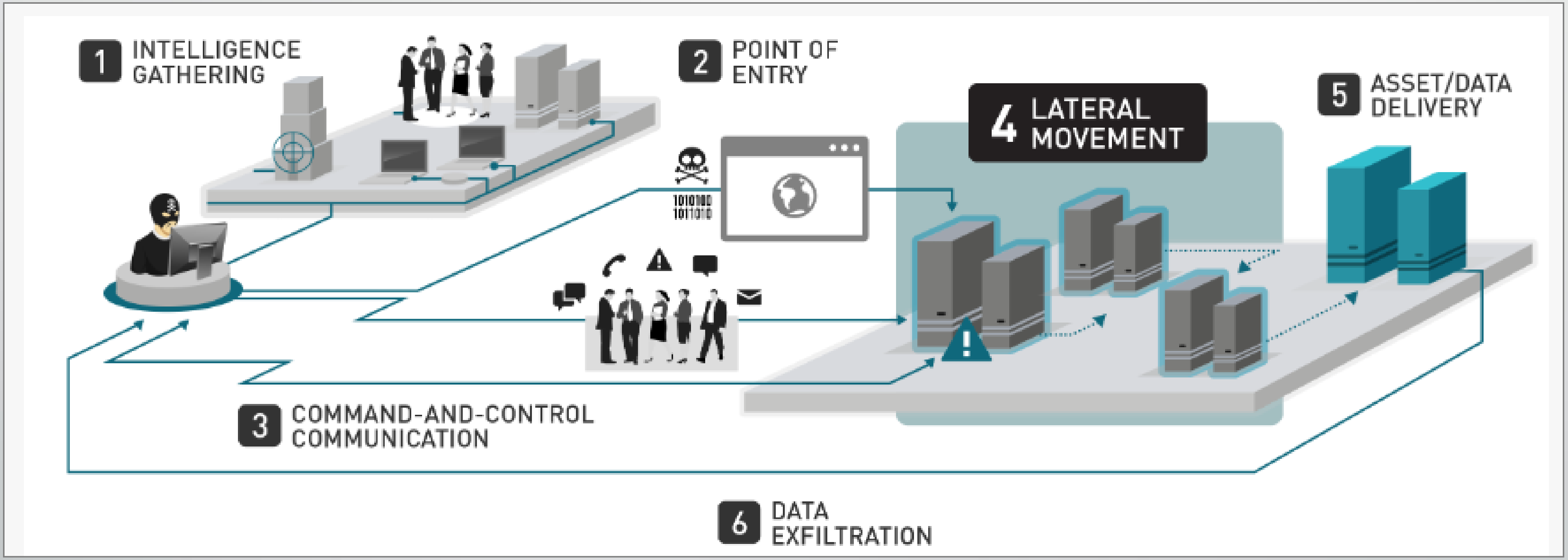
- Security enthusiast.
- Red teaming and penetration testing.

- **Twitter:** @truneski
- **Website:** truneski.github.io
- **Email:** vincetrune<at>gmail.com

Why we're here

- The **structure of a cyber attack** from initial reconnaissance to objective completion.
- We'll outline common Tools, Techniques and Procedures (TTPs) used by malicious actors in the wild today.
- Focus is on **methodology**, not motive.
- Methodologies become more advanced as you move up the **threat pyramid**, but the general theme of the most common attacks remains the same.

Attack Phases

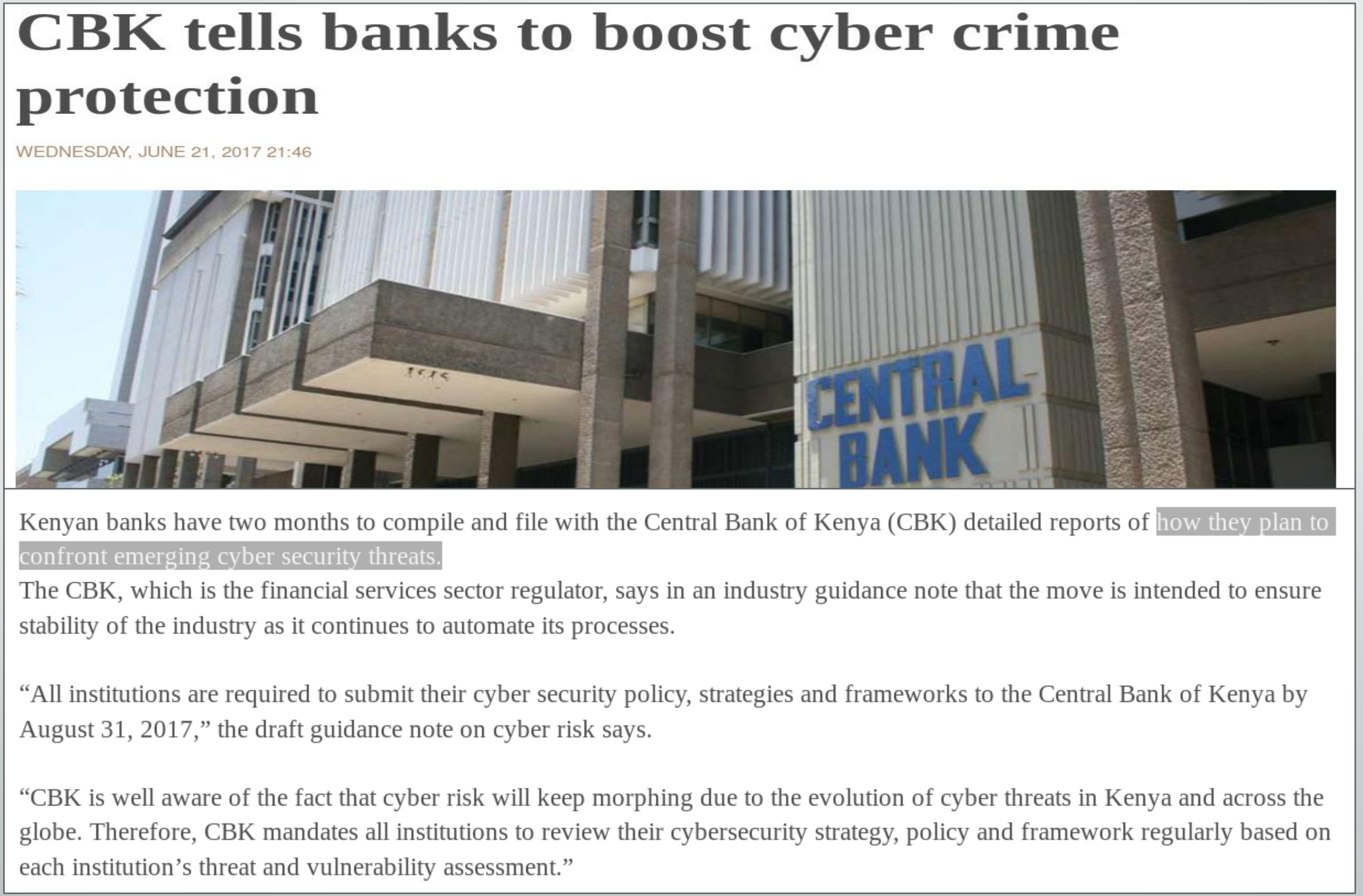


Our Target

Iron Bank

- The **Iron Bank** is a bank in the Free City of Braavos.
- It is arguably the most powerful financial institution in the 7 kingdoms.

Why Banks?



CBK tells banks to boost cyber crime protection

WEDNESDAY, JUNE 21, 2017 21:46

Kenyan banks have two months to compile and file with the Central Bank of Kenya (CBK) detailed reports of how they plan to confront emerging cyber security threats.

The CBK, which is the financial services sector regulator, says in an industry guidance note that the move is intended to ensure stability of the industry as it continues to automate its processes.

“All institutions are required to submit their cyber security policy, strategies and frameworks to the Central Bank of Kenya by August 31, 2017,” the draft guidance note on cyber risk says.

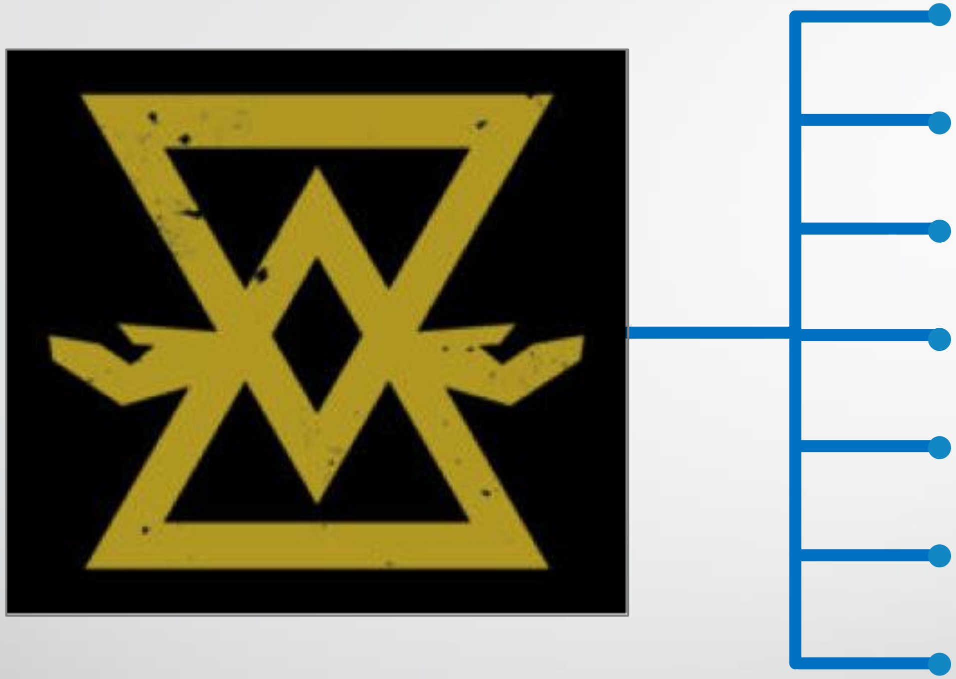
“CBK is well aware of the fact that cyber risk will keep morphing due to the evolution of cyber threats in Kenya and across the globe. Therefore, CBK mandates all institutions to review their cybersecurity strategy, policy and framework regularly based on each institution’s threat and vulnerability assessment.”

Iron Bank Defenses

The Usual Suspects

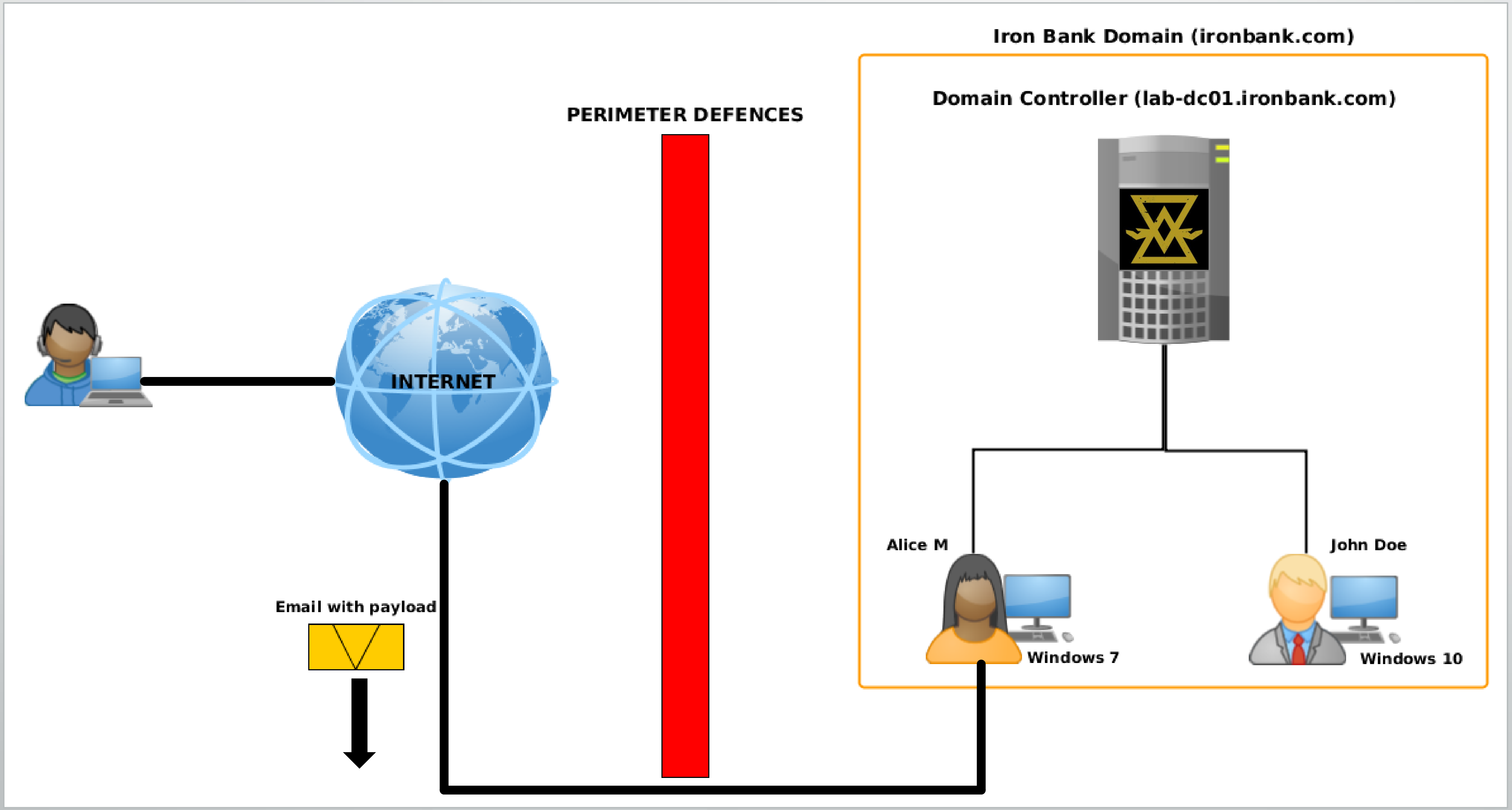
- Firewalls.
- Monitoring solutions e.g. SIEMs.
- Site blocking.
- Antivirus.
- Okay-ish patch cycle.
- Strong user account & password policies.
- Security staff (blue team).

1. Recon



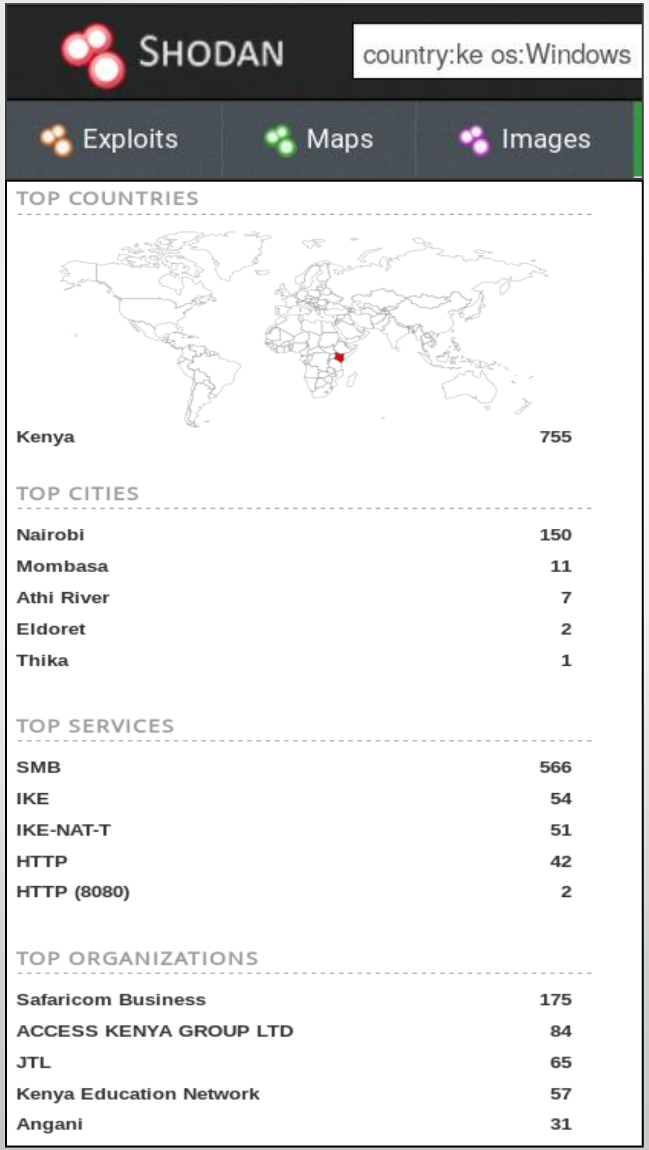
- Domains & IP ranges.
- Websites/web applications.
- Infrastructure.
- Locations.
- ***People.***
- ***Emails.***
- Social media.

Our Scenario



DEMO

2. Exploitation - Service Exploitation



country:ke os:Windows

TOP COUNTRIES

Kenya	755

TOP CITIES

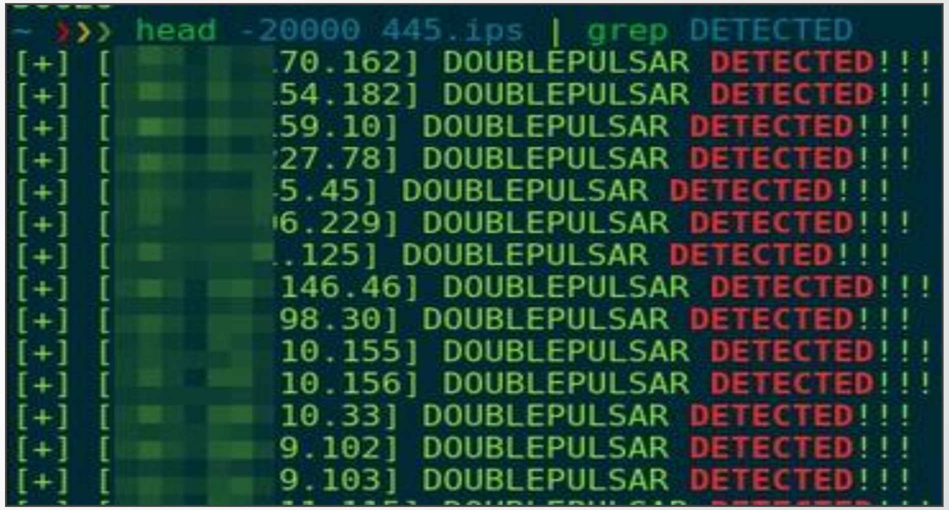
Nairobi	150
Mombasa	11
Athi River	7
Eldoret	2
Thika	1

TOP SERVICES

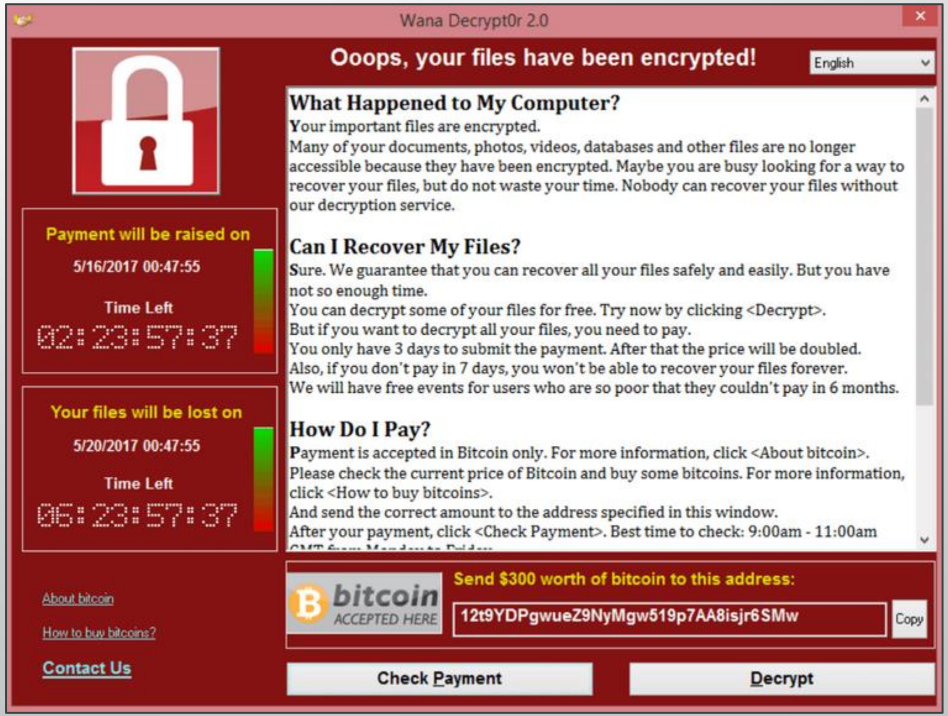
SMB	566
IKE	54
IKE-NAT-T	51
HTTP	42
HTTP (8080)	2

TOP ORGANIZATIONS

Safaricom Business	175
ACCESS KENYA GROUP LTD	84
JTL	65
Kenya Education Network	57
Angani	31



```
~ ))) head -20000 445.ips | grep DETECTED
[+] [[redacted]70.162] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]54.182] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]59.10] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]27.78] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]5.45] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]6.229] DOUBLEPULSAR DETECTED!!!
[+] [[redacted].125] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]146.46] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]98.30] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]10.155] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]10.156] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]10.33] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]9.102] DOUBLEPULSAR DETECTED!!!
[+] [[redacted]9.103] DOUBLEPULSAR DETECTED!!!
```



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

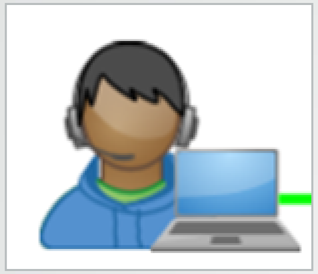
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

2. Exploitation - Emails

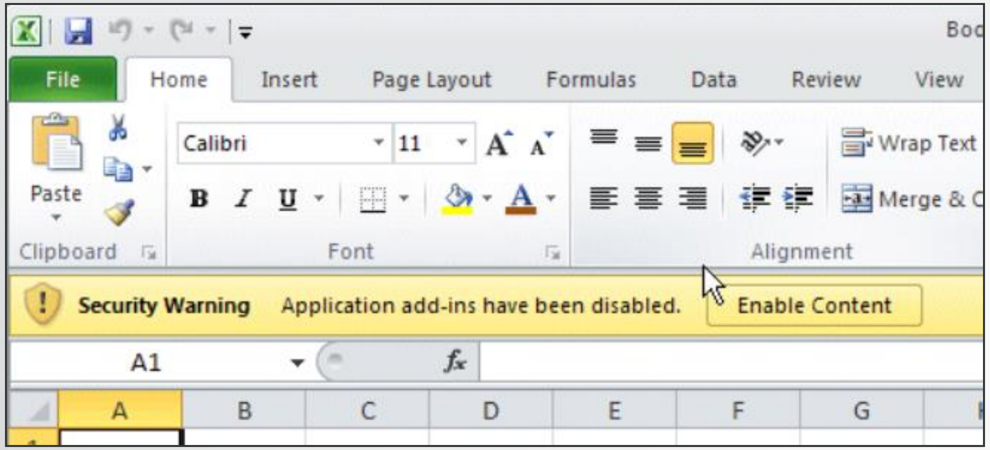


Bad Guy – badguy@krcc.co.ke

Alice – alice@krcc.co.ke

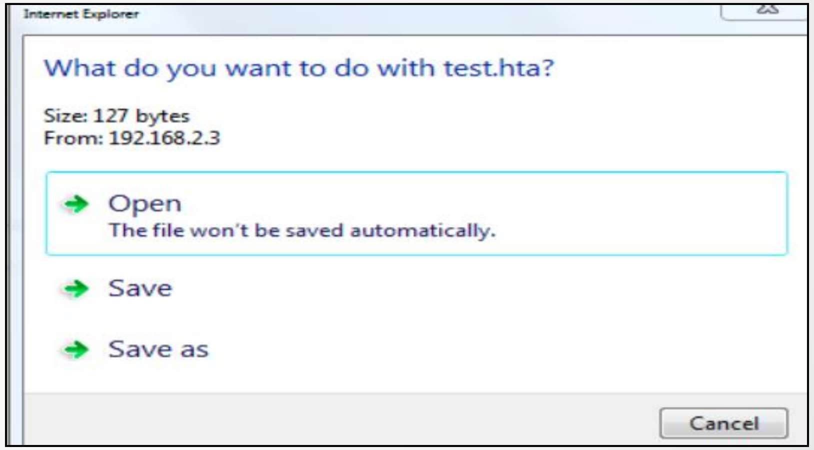
2. Exploitation - Emails

Macros



Security Warning Application add-ins have been disabled. Enable Content

HTA

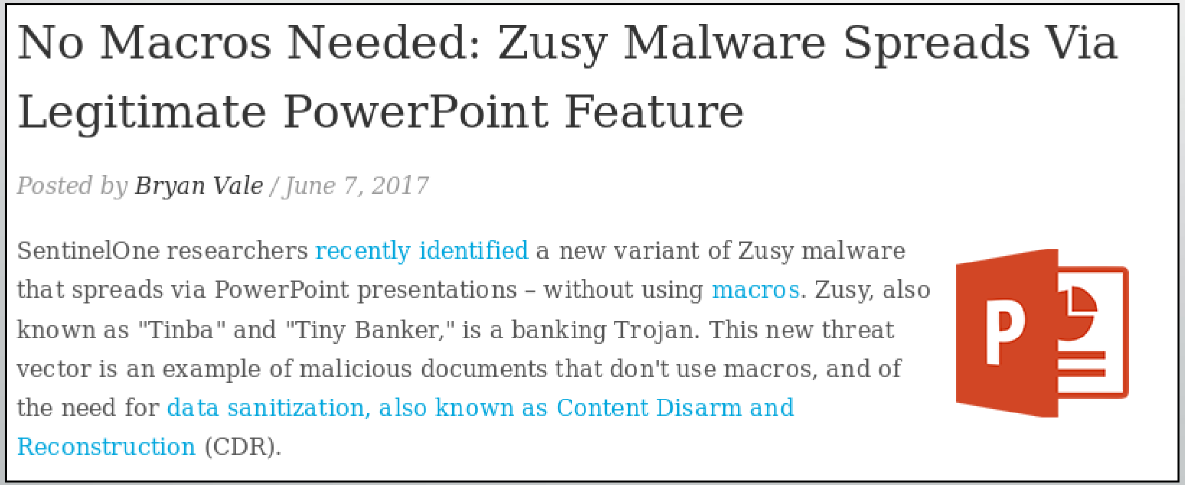


What do you want to do with test.hta?

Size: 127 bytes
From: 192.168.2.3

The file won't be saved automatically.

PowerPoint



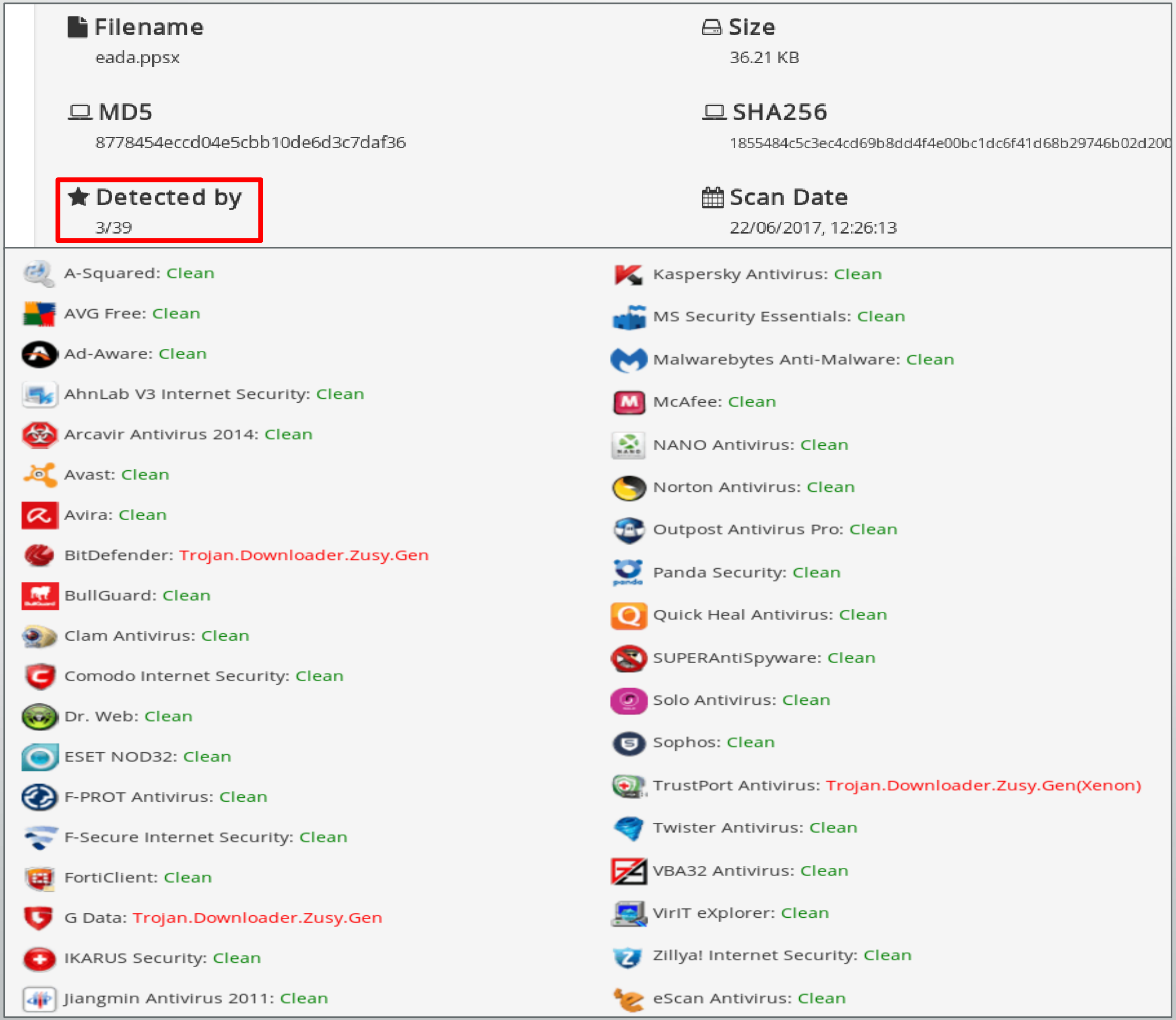
No Macros Needed: Zusy Malware Spreads Via Legitimate PowerPoint Feature

Posted by Bryan Vale / June 7, 2017

SentinelOne researchers recently identified a new variant of Zusy malware that spreads via PowerPoint presentations – without using macros. Zusy, also known as "Tinba" and "Tiny Banker," is a banking Trojan. This new threat vector is an example of malicious documents that don't use macros, and of the need for data sanitization, also known as Content Disarm and Reconstruction (CDR).

No Powershell

Zusy Detection



Filename
eada.ppsx

Size
36.21 KB

MD5
8778454eccd04e5cbb10de6d3c7daf36

SHA256
1855484c5c3ec4cd69b8dd4f4e00bc1dc6f41d68b29746b02d200

Detected by
3/39

Scan Date
22/06/2017, 12:26:13

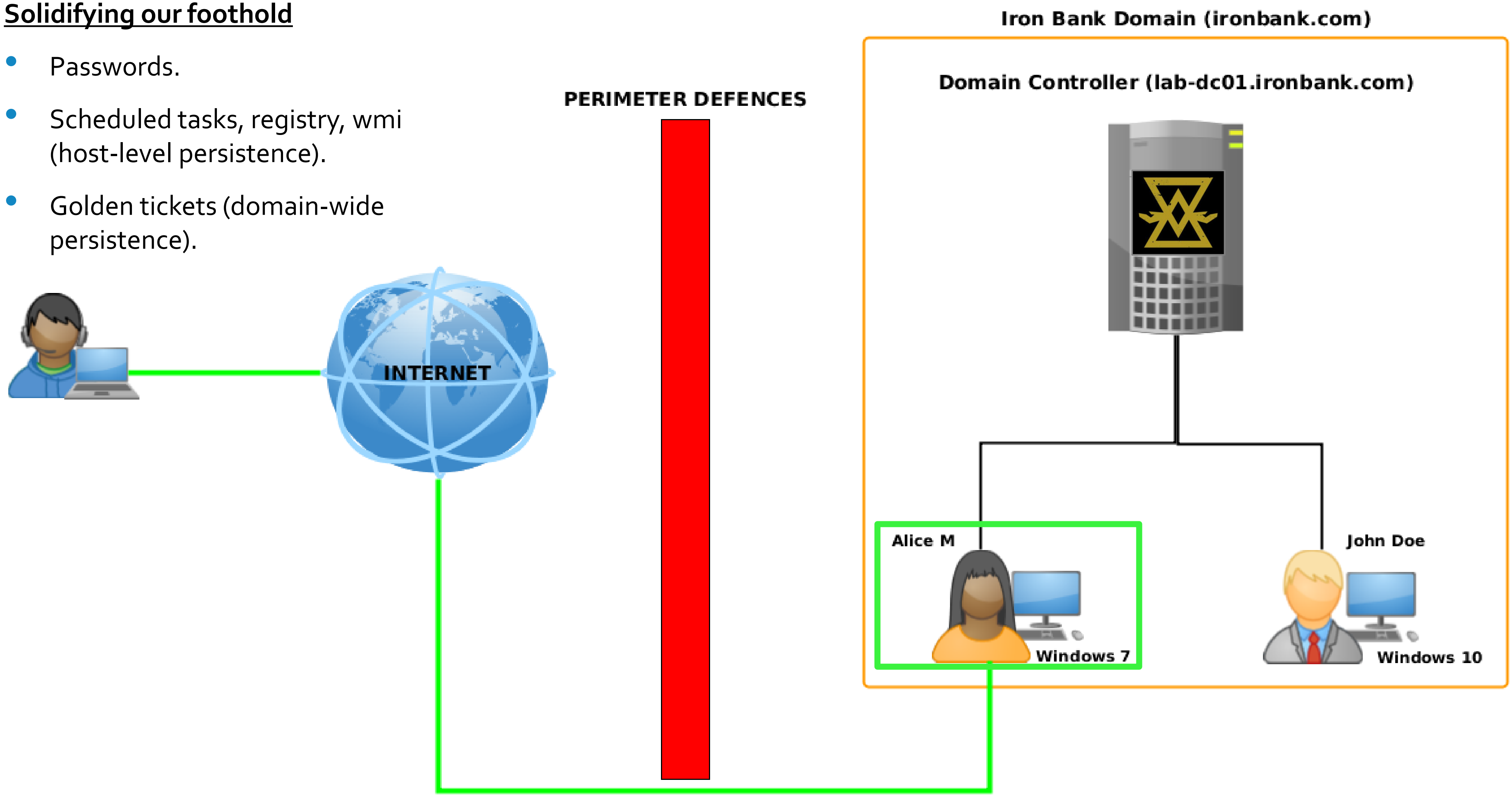
A-Squared: Clean
AVG Free: Clean
Ad-Aware: Clean
AhnLab V3 Internet Security: Clean
Arcavir Antivirus 2014: Clean
Avast: Clean
Avira: Clean
BitDefender: Trojan.Downloader.Zusy.Gen
BullGuard: Clean
Clam Antivirus: Clean
Comodo Internet Security: Clean
Dr. Web: Clean
ESET NOD32: Clean
F-PROT Antivirus: Clean
F-Secure Internet Security: Clean
FortiClient: Clean
G Data: Trojan.Downloader.Zusy.Gen
IKARUS Security: Clean
Jiangmin Antivirus 2011: Clean
Kaspersky Antivirus: Clean
MS Security Essentials: Clean
Malwarebytes Anti-Malware: Clean
McAfee: Clean
NANO Antivirus: Clean
Norton Antivirus: Clean
Outpost Antivirus Pro: Clean
Panda Security: Clean
Quick Heal Antivirus: Clean
SUPERAntiSpyware: Clean
Solo Antivirus: Clean
Sophos: Clean
TrustPort Antivirus: Trojan.Downloader.Zusy.Gen(Xenon)
Twister Antivirus: Clean
VBA32 Antivirus: Clean
VirIT eXplorer: Clean
Zillya! Internet Security: Clean
eScan Antivirus: Clean

2. Exploitation - USB

3. Persistence

Solidifying our foothold

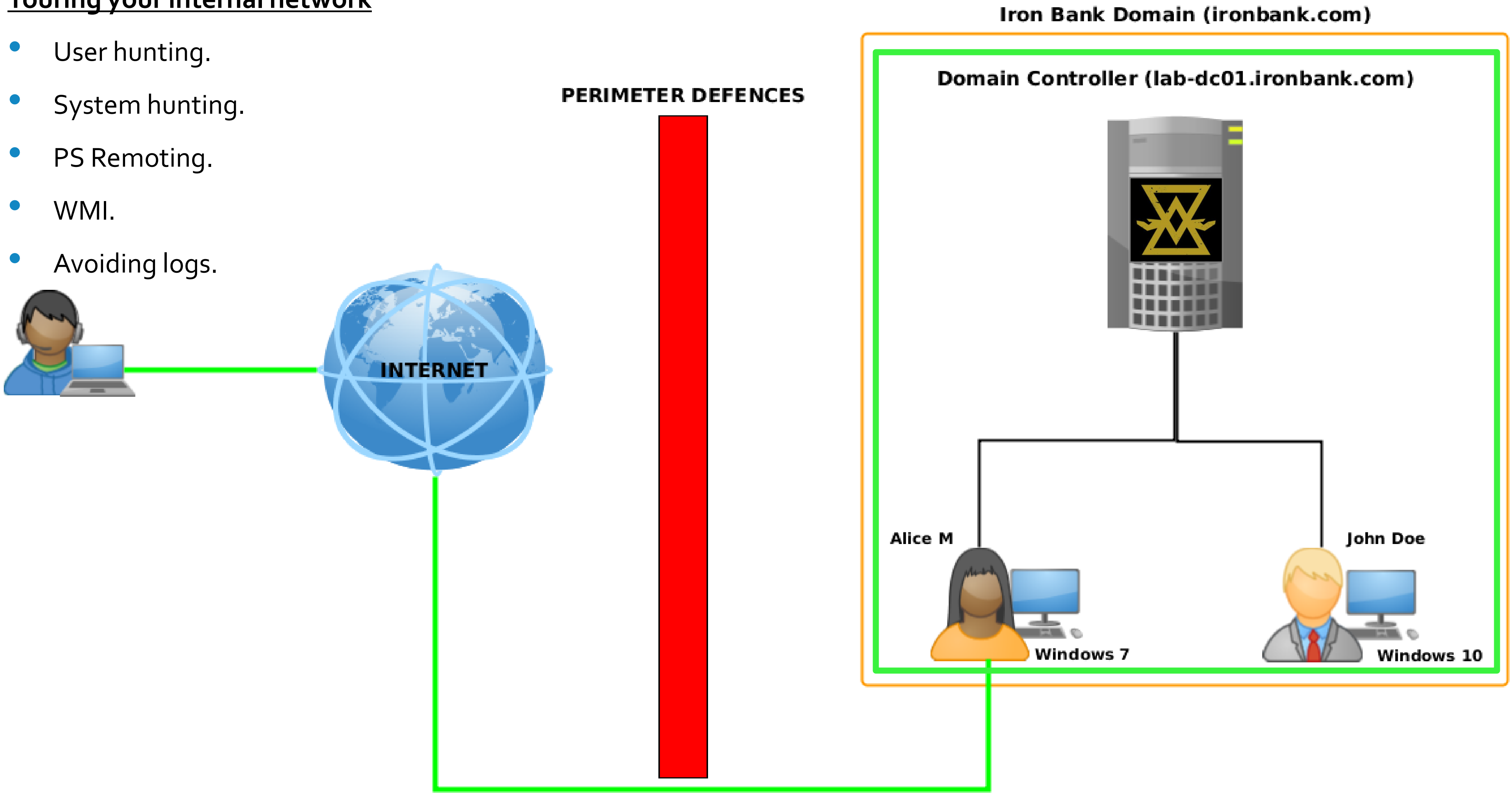
- Passwords.
- Scheduled tasks, registry, wmi (host-level persistence).
- Golden tickets (domain-wide persistence).


Iron Bank Domain (ironbank.com)
Domain Controller (lab-dc01.ironbank.com)
PERIMETER DEFENCES
INTERNET
Alice M
Windows 7
John Doe
Windows 10

4. Lateral Movement

Touring your internal network

- User hunting.
- System hunting.
- PS Remoting.
- WMI.
- Avoiding logs.


Iron Bank Domain (ironbank.com)
Domain Controller (lab-dc01.ironbank.com)
PERIMETER DEFENCES
INTERNET
Alice M
Windows 7
John Doe
Windows 10

Golden Ticket

WONKA'S
GOLDEN TICKET

GREETINGS TO YOU,THE LUCKY FINDER OF THIS GOLDEN TICKET. FROM MR. WILLY WONKA!...

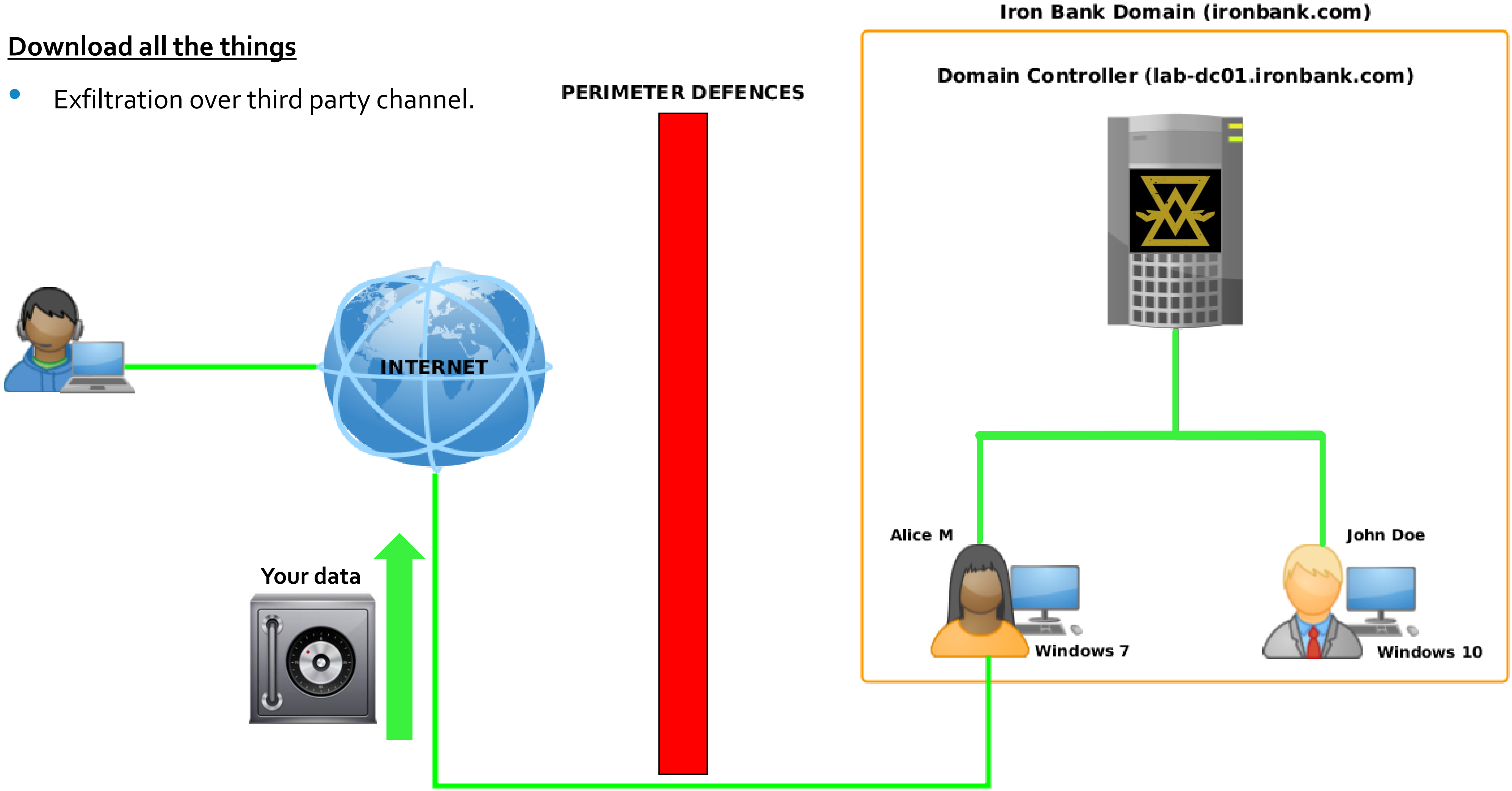
PRESENT THIS TICKET AT THE FACTORY GATES AT TEN O'CLOCK IN THE MORNING OF THE FIRST DAY OF OCTOBER AND DO NOT BE LATE. YOU MAY BRING WITH YOU ONE MEMBER OF YOUR OWN FAMILY... AND ONLY ONE... BUT NO ONE ELSE........

In your wildest dreams you could not imagine the marvelous SURPRISES *that await* YOU!

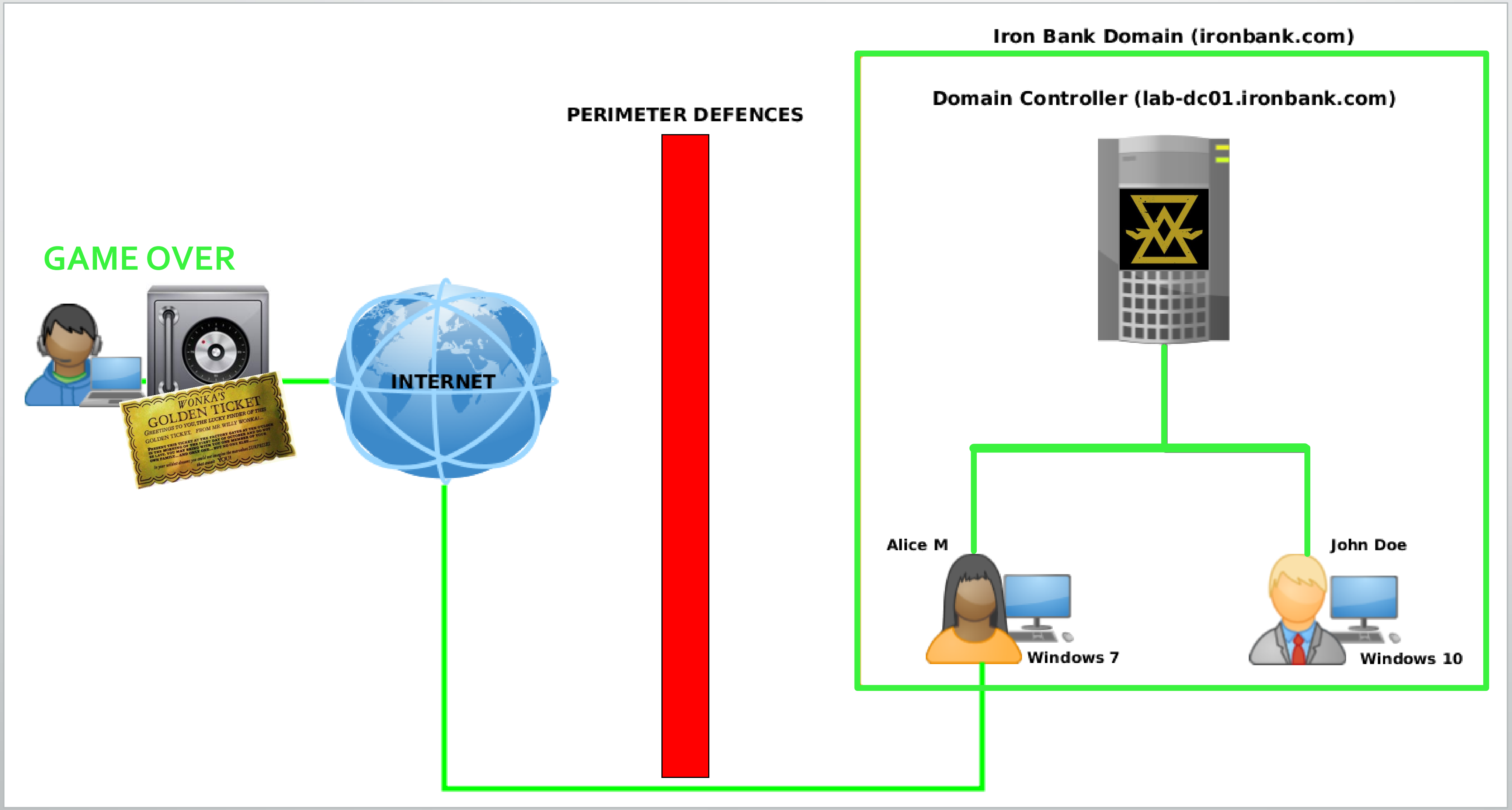
5. Data Exfiltration

Download all the things

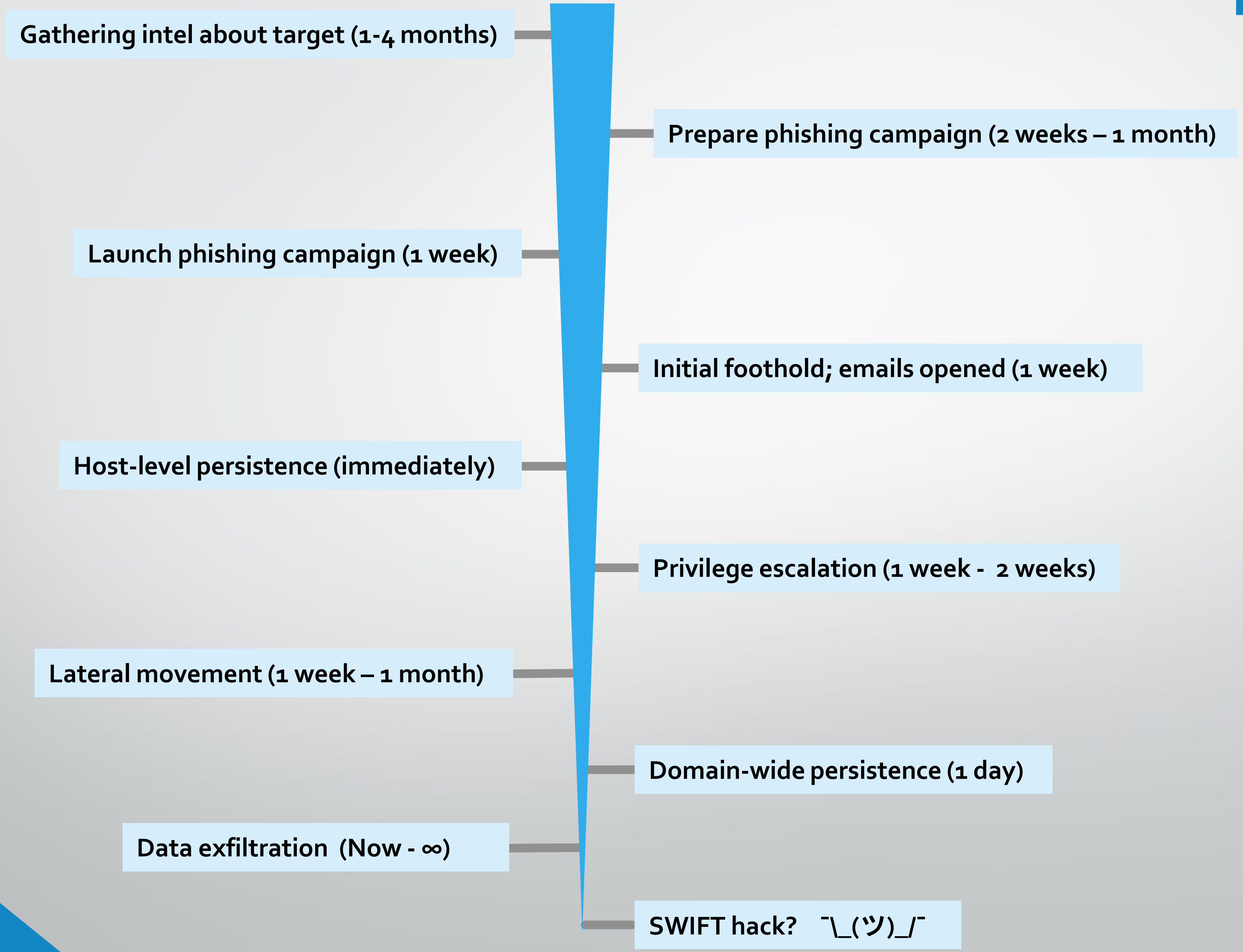
- Exfiltration over third party channel.


Iron Bank Domain (ironbank.com)
Domain Controller (lab-dc01.ironbank.com)
PERIMETER DEFENCES
INTERNET
Your data
Alice M
Windows 7
John Doe
Windows 10

Endgame


Iron Bank Domain (ironbank.com)
Domain Controller (lab-dc01.ironbank.com)
PERIMETER DEFENCES
GAME OVER
WONKA'S GOLDEN TICKET
INTERNET
Alice M
Windows 7
John Doe
Windows 10

Timeline



Gathering intel about target (1-4 months)

Prepare phishing campaign (2 weeks – 1 month)

Launch phishing campaign (1 week)

Initial foothold; emails opened (1 week)

Host-level persistence (immediately)

Privilege escalation (1 week - 2 weeks)

Lateral movement (1 week – 1 month)

Domain-wide persistence (1 day)

Data exfiltration (Now - ∞)

SWIFT hack? ¯_(ツ)_/¯

How do we stop it?

Phase	Mitigations/Recommendations
Exploitation	▪ Less obsession with perimeter security. Assume compromise. ▪ They will get in. Will you know when they do? What can you do to stop it? ▪ Patching, patching, patching. ▪ Train users to identify threats. ▪ Endpoint security & real-time monitoring; workstations are their way in. ▪ Invest in your security team.
Persistence	▪ Limit domain admins. Limit where domain admins can login (e.g. only to DCs) ▪ Attackers need DC access to create Golden Tickets, don't let them get to your DC. ▪ Do your users have local admin rights? ▪ Invest in your security team.
Lateral Movement	▪ Flat domain for your entire organisation? Nope. ▪ Network isolation. ▪ Logon restrictions. ▪ Event/process monitoring. ▪ Application whitelisting. ▪ Invest in your security team.
Data exfiltration	▪ Network monitoring. ▪ Network filtering. ▪ Network segmentation. ▪ Network flow baselines and anomalous activity. Can you tell the difference? ▪ Process monitoring. Powershell talking to Dropbox? Why? ▪ Invest in your security team.

…this is just the tip of a very large iceberg. To put it simply; invest in your security team.

THANK YOU