Red Team Apocalypse

Derek Banks (@0xderuke)

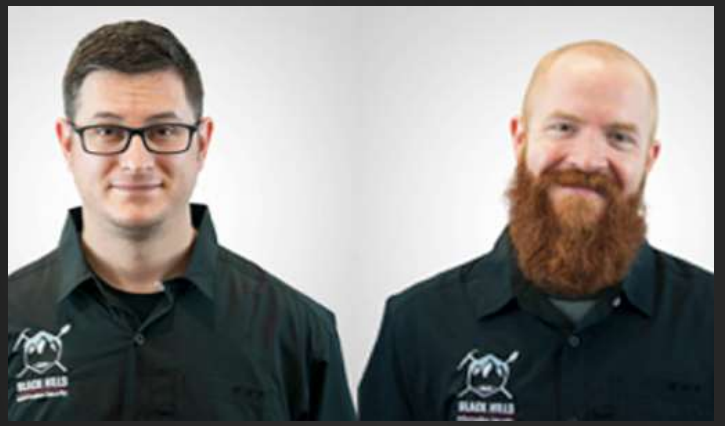
Beau Bullock (@dafthack)

About

- Your organization has a vulnerability management program and regularly patches
- You implemented application whitelisting and network egress controls
- The latest round of pen testers didn't find anything too concerning
- You have the latest Cyber Anti APT Blinky box appliance
- Your organization's critical database is being sold on the dark web.
- What happened?!

About Us

- Pentesters at Black Hills Information Security
- Have a number of SANS, OffSec, and other certs…
- CitySec Meetup Organizers
  - CigarCitySec – (Tampa, FL)
  - CitrusSec – (Orlando, FL
  - TidewaterSec – (Hampton, VA)
- Tradecraft Security Weekly and Hacker Dialogues podcasts
- Avid OWA enthusiasts



Original Pentest Apocalypse

- Vulnerability Management Program
- Group Policy Preferences
- Widespread Local Administrator Account
- Weak Passwords (Password Spraying)
- Over Privileged Users
- Sensitive Data in File Shares
- Intranet Information Disclosure
- NetBios and LLMNR Poisoning
- Local Workstation Privilege Escalation

Red Team vs Pen Test

- Penetration test goals tend to be find as many vulnerabilities in the allotted time
  - Use COTS tools automated tools like vulnerability scanners
  - Generally not concerned with alerting the blue team
- Red teams engagements model real world adversaries and are focused on achieving a goal
  - May use custom written malware and tools
  - Generally attempt to be stealthy and not alert the blue team

Red Team Methodology

- Reconnaissance
- Compromise
- Persistence
- Command and Control
- Asset Discovery
- Privilege Escalation
- Lateral Movement
- Actions on Objectives

Calendar Event Injection

Google Calendar Event Injection

- Silently inject events into calendars
- Creates urgency via reminders
- Include a link to a fake agenda
- An email isn't necessary, simply add a Google user to an event and select checkbox to not notify them
- Google will automatically add it to their calendar
- This presents a unique phishing situation

Google Calendar Event Injection

- A few ideas:
  - Include a link to a conference call site but have it pointing to a credential collection page
  - Include a malicious “agenda”
  - Have victims navigate to a fake Google Auth page and collect creds
- Gets more fun with Google API
  - **It’s possible to make it look like they already accepted the invite!**
  - **This completely bypasses the setting in G-calendar for not auto-adding events.**

Email Attacks

Business Email Capture

- Externally accessible email portals are a target
  - Even if they are 2FA
  - OWA I'm looking at you
  - Cloud services are a target too (Gmail, O365, etc.)
- Pen testers may overlook email systems as a target
- Threat actors (and Red Teamers) do not
- Email is a huge resource for an attacker to learn more about your environment

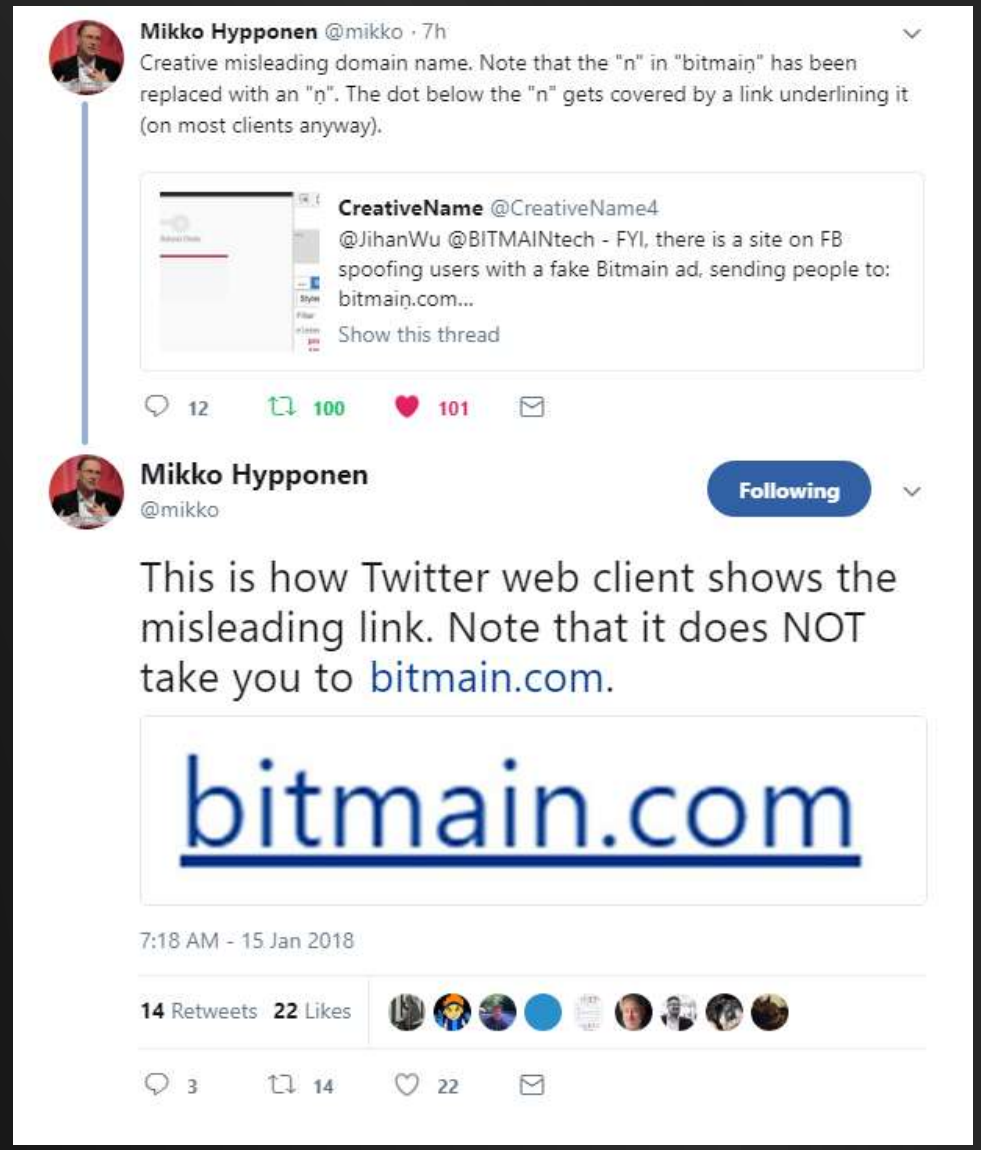
Business Email Capture

- MailSniper
  - https://github.com/dafthack/MailSniper
- Domain / Username enumeration
- Password Spraying
- GAL Download
- Open Inbox delegation discovery
- Email searching for terms like passwords, 2FA codes, etc…
- Bypasses some 2FA products by connecting to EWS instead of OWA

Unicode Domain Names

Unicode Domain Names

- Use of domain names that include unicode characters such as letters with a dot (.) under them like: ṇ
- Creates a really great look-alike domain for phishing
- The dot gets completely hidden when hyperlinked with a line underneath
- Gotta be careful with some spam filters though



Expired Categorized Domains

Expired Categorized Domains

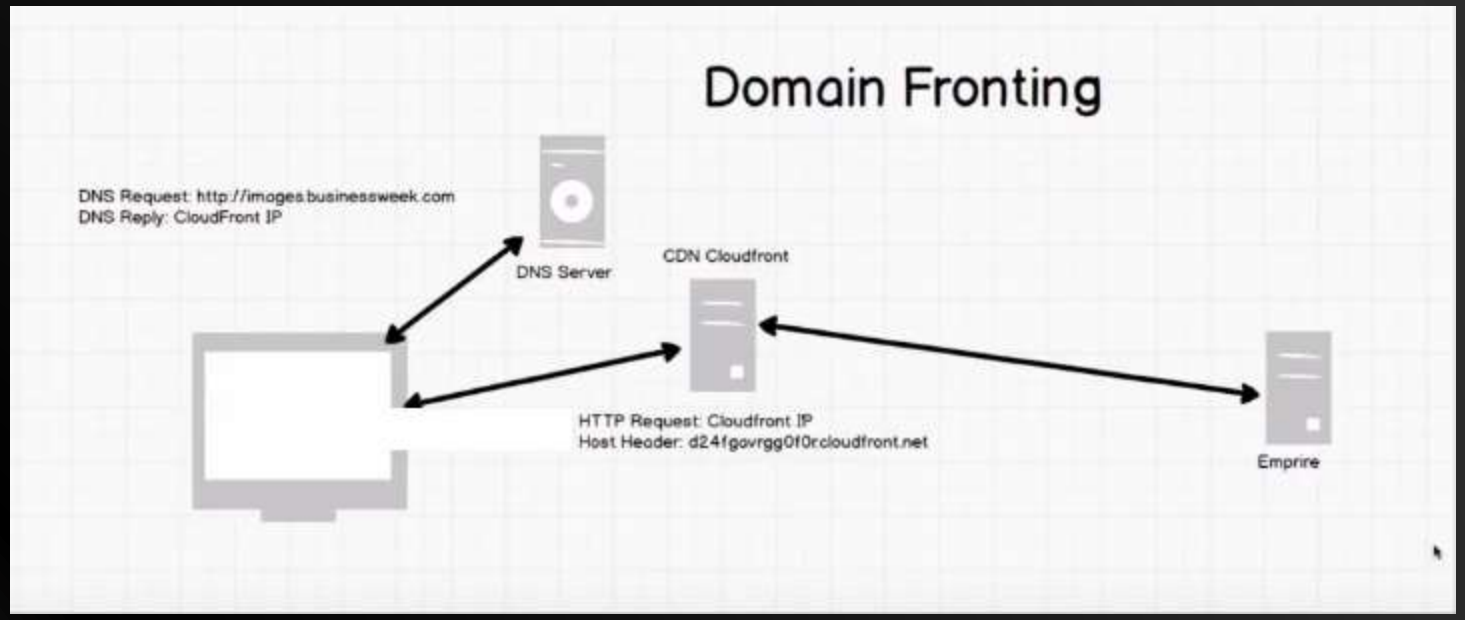
- Technique used to circumvent categorization web proxy blocks for C2
- Uses previous categorization for some length of time
- Trivial to find
  - expireddomains.net
  - Domainhunter.py
- Simulates using a compromised 3rd party website

Domain Fronting

Domain Fronting

- Another technique used to circumvent web proxy restrictions for C2
- Hides the true endpoint of an HTTP connection
- Initial target domain for the traffic redirects to secondary host
- Can use a Content Delivery Network such as AWS Cloudfront
- Can be difficult to detect and block

Domain Fronting



Hashes Just Want to Be Cracked

Kerberoasting

- Ability for any domain user to query the domain for a Service Principal Name for an account associated with running a service
- A request to authenticate over Kerberos results in a service ticket where a portion is encrypted with the service account hash
- Effectively any domain user can get a hash of a service account with an SPN and take the resulting ticket offline and attempt to crack it

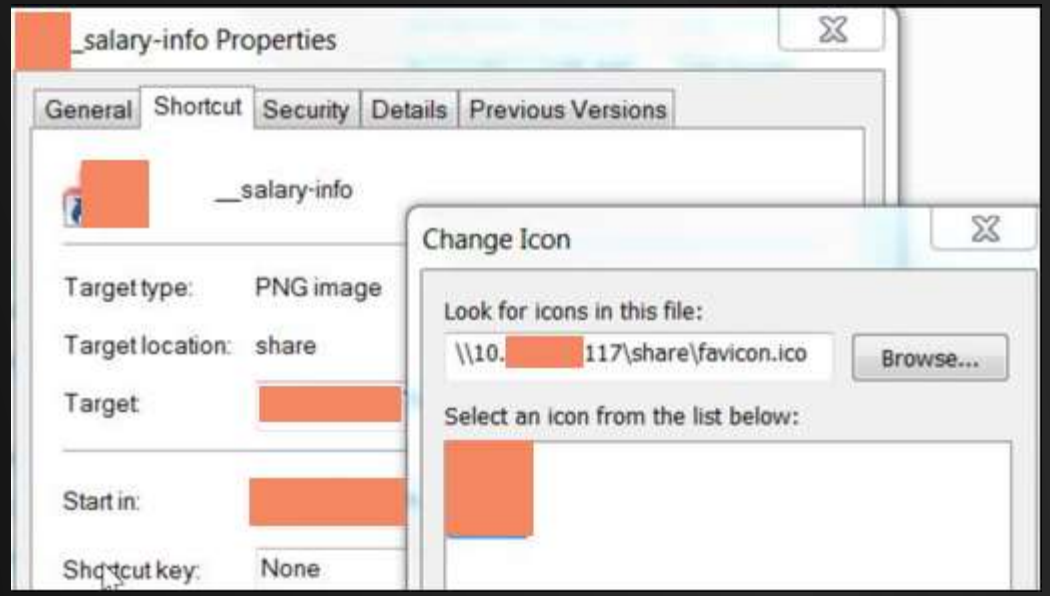
Evil Twin Wireless Attack

- Evil Wireless AP that uses the same ESSID as the target AP
- Goal is to trick a user into joining the evil AP and gather the NetNTLMv2 hash from the authentication attempt
- Eaphammer from s0lst1c3
  - https://github.com/s0lst1c3/eaphammer
- Hostapd-wpe
  - https://github.com/OpenSecurityResearch/hostapd-wpe
- Aircrack suite

Weaponized LNK File

- Place shortcut file located on a commonly used public share
- Icon for shortcut points back a UNC location on attacker system

- SMB Listener on attacker controlled system
- Can use Inveigh for the listener
  - https://github.com/Kevin-Robertson/Inveigh
- Gather NetNTLMv2 hashes



Onsite Attacks

NAC Bypass

- Spoof another device
  - Find a printer or VOIP phone; Spoof MAC and/or IP
  - Voiphopper to hop VLAN's
  - For Wi-Fi NAC spoof MAC and User Agent of connected device
- Layer 2 and 3 NAT device
  - Helps avoid triggering port security rules on 802.1X
  - Device spoofs both sides of wire
  - Passively learns MAC addresses

Dropbox

- Fully functional pentesting device to leave at onsite
- Persistent reverse SSH tunnels
- Can be controlled over WiFi
- Relatively unnoticeable
- ODROID-C2 build instructions here:
  - https://www.blackhillsinfosec.com/how-to-build-your-own-penetration-testing-drop-box/

PXE Booting Attacks

- Obtain the “Golden” image from the network
- Set VM to “Boot from network”, boot VM, and get the image
- Mount image & profit
  - Steal Admin hashes
  - Set local admin pass pre-boot
  - Overwrite Sticky keys (sethc.exe)

Post Exploitation

PowerUp SQL

- PowerShell tool for attacking MSSQL
  - https://github.com/NetSPI/PowerUpSQL
- SQL Server discovery
- Weak configuration auditing
- Privilege escalation
- Data sample searches
- OS command injection
- All at scale across the enterprise

Living off the Land

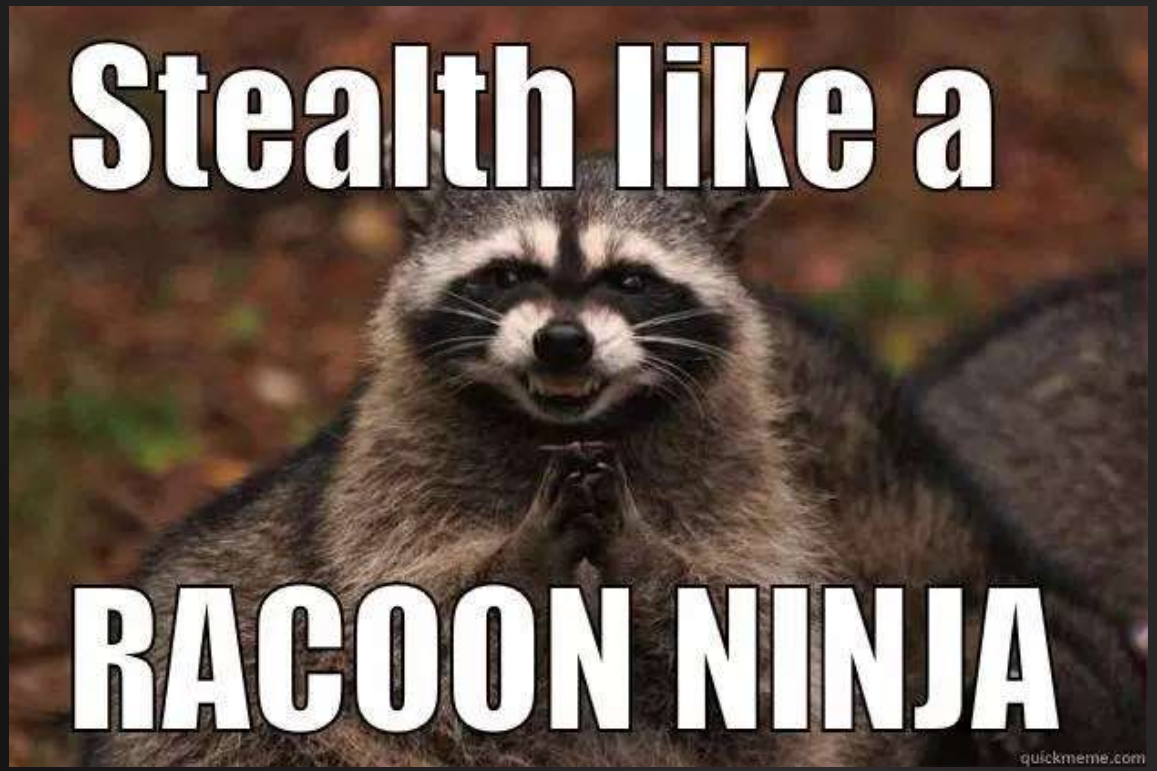
- Using built in Windows tools to avoid dropping malware
- Internal user and group recon
- Remote file listing and copying data
- Remote process spawning
- Lateral movement

Living of the Land

- Net commands
  - net groups “DOMAIN ADMINS” /DOMAIN
- Listing files on remote hosts
  - dir \\host\C$\files
- WinRM to run remote commands (port 5985)
  - Invoke-Command -ComputerName -ScriptBlock {Command Here}

Stealthy Host/Domain Enumeration

- More and more AV, behavioral analysis, app whitelisting, etc. products are starting to either block or alert on built-in system commands
  Ex. net, ipconfig, whoami, netstat, etc.
- HostRecon PowerShell instead of built-in commands
  - https://github.com/dafthack/HostRecon
- Combine with PowerShell Without PowerShell technique for added bonus



Detection and Prevention

Solid Systems Administration

- Systems and software inventory (yes, CSC Top 20 are useful)
- Workstations should never talk to workstations - client to server communication only
  - Windows firewall or Private VLANS
- Baseline images with GPO enforcement
- All inbound and outbound network traffic go through an application proxy system
  - Any exceptions for direct outbound communication are by documented exception only

Enforce Good User Behavior

- Change every inbound email subject line with a tag such as (External):
- Inform your users that any email with that tag needs extra scrutiny
- Minimum of 15 characters for any domain account password
  - If you have to compromise to sell it to the business, no complexity requirements and 6 month change interval
- Consider additional credential defenses
  - Commercial offerings available
  - CredDefense Toolkit for Free
    - https://github.com/creddefense

Host Log Consolidation

- Consolidate key logs from endpoints, servers, and appliances to a central location
- Specifically monitor PowerShell and process execution
- Sysmon a powerful and free option for gaining insight into host based activity
- Once the logging foundation is in place, alert on “abnormal commands” like net commands
- Can be done on the cheap:
  - https://www.blackhillsinfosec.com/end-point-log-consolidation-windows-event-forwarder/

Network Logging

- NetFlow, Bro, or Full Packet Capture?
  - Depends on your budget and staff capabilities
- Bro is a good balance between NetFlow 5-Tuple and Full Packet Capture mass storage requirements
- Out of the box captures common protocols into text based files
- Can provide an amount of visibility into SSL traffic without breaking SSL
  - Abnormal certificate information
  - SSL fingerprinting - JA3 project - https://github.com/salesforce/ja3
- Beacon detection with RITA (AIHunt)
  - https://www.blackhillsinfosec.com/projects/rita/

Red Team Prepper

- Don’t wait on the Red Team prepare on your own
- Use @vysecurity’s Red Team Tips to find techniques to try to detect
  - https://github.com/vysec/RedTips
- MITRE ATT&CK Framework for threat actor techniques
  - https://attack.mitre.org/wiki/Main_Page
- Red Canary’s Atomic Red Team - portable scripts to test ATT&CK framework
  - https://github.com/redcanaryco/atomic-red-team

About that Bypass Technique

- Recently some products have been getting a little better…
- But they still seem to be getting better at catching pen testers and common tools
- And then sometimes its just stupid simple to get past a well known security product

```
derek@db-2017-350-2:~$ ncat -nlvp 8888
Ncat: Version 7.01 ( https://nmap.org/ncat )
Ncat: Listening on :::8888
Ncat: Listening on 0.0.0.0:8888
Ncat: Connection from [redacted].
Ncat: Connection from [redacted]:50716.
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\dbanks\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>whoami
whoami
[redacted]\dbanks
```

Summary and Conclusions

- Black Hills Information Security
  - http://www.blackhillsinfosec.com
  - @BHInfoSecurity
- Beau Bullock @dafthack
- Derek Banks @deruke
- Questions?