Osaka, Japan

VOODOO

DAVID BRYAN, CODE NAME: VIDEODIAN

KUMSAN WANTS OUR TEAM TO TEST BEYOND THE PHYSICAL, THOUGH. LET'S RUN THE ETERNAL BLUE EXPLOIT...

AND SET EVILMOG IN THE MIX.

DUSTIN, CODE NAME: EVILMOG

GOT IT. TIME TO RELEASE CRACKEN.

TREY, TREY, TREY, TREY

“PHYSICAL LAYER HAS BEEN COMPROMISED.”

“AND WE'RE IN MISSION ACCOMPLISHED.”
Several months later.
Austin, Texas

CHARLES HENDERSON
CODE NAME: ANGUS

THE AVA ARE FINALLY COMING OUT.

RIGHT, EVERY HALF-DECENT CRIMINAL WILL BE GUNNING FOR US UNLESS WE GET TO THEM FIRST.

GRRRRR

IMAGINE WHAT THE WRONG PERSON COULD DO WITH THE RIGHT ACCESS. THAT'S WHY I WANT YOU—WHAT IS IT YOU ALWAYS SAY? HACKING ANYTHING...

WHERE'S THE FUN IN THAT, XIMENA? BESIDES, TOKYO IS ONE OF MY FAVORITE CITIES.

WHERE ARE WE AT, KRIS?

NEEDS THE WORKS: APPLICATION, NETWORK, HARDWARE, AND HUMAN.

WE'RE LAUNCHING THE WORLD'S FIRST FLEET OF FULLY AUTONOMOUS VEHICLES. YOU'VE GOT TO TEST MY SECURITY TEAM IN EVERY WAY POSSIBLE.

KRIS, SAFE
CODE NAME: SAFIRE

CLIENT: XIMENA COMPANY

...TO SECURE EVERYTHING.
Hey, team! We've got a job: our biggest one yet.

Cris Thomas, code name: Space Rogue

Steve Ocepek, code name: Nesteeve

Thomas Mackenzie, code name: Mac

Stephanie Carruthers, code name: Snow

Alberta, Canada

Evillog

Accra, Ghana

Dubai, United Arab Emirates

Salt Lake City, Utah

Washington, D.C.

Cleveland, Ohio

Manchester, England

California

Catherine Norcom, code name: Q

Stephen Asamoah, code name: Opphi

Leonidas Kouvartakis, code name: Zeus
One week later.

Stephen: How are we doing on... Has our SSO got anything popped yet?

X-Force: Phishing has been unsuccessful.

Stephen: Ximena has a great response team. They keep detecting us and shutting us down.

We've only got three weeks before the AU announcement.

I know there's something we're missing. That some hacker out there won't.

Application Layer
  Spaghetti Code
  Redirectors
  Environment Restrictions
  Social Engineering
  Backend System

Team, our clients give us the unscaleable wall because they know we're the best.

But is any of that working yet?
**Manchester, England**

TMac, the auto specialist.

**Chicago, Illinois**

Snow, the social engineering expert.

**Alberta, Canada**

Evilmog, the Wildcard.

**California**

Q, the Thingmaker.

**Texas**

H4CK3R

---

**SHE**

So dig deep and get creative. Let's make it happen.

**ANALOG DEEP DIVE**

Chris?

**HA HA**

TMac.

They did a massive profile on the CEO of...

**THE GEOFENCING**

In this model, isn't very secure...

**KLIP KLIP**

---

**THANKS AGAIN FOR HELPING WITH OUR SURVEY! GOOD LUCK WITH THE REST OF YOUR INTERNSHIP.**

**NO PROB.**

**EVER HEARD OF BIOGLASS IMPLANTS?**

**WHAT?**

**LIKE PROGRAMMABLE CHIPS YOU INJECT INTO YOUR BODY?**

**OUCH!**

**SORRY! BIG IMPLANTS, huh?**

**SOUNDS KINDA CRAZY.**

---

**THEY**

---

**NEXT TO**

HQ.

**GOTTA PUT IN AN ORDER FOR DONUT THURSDAYS.**

Ah, nearly forgot!
@Charles the team will be in Chicago at [redacted] HQ for the engagement. Everything’s set for next week.

Perfect. @Videoman @ Hullhog @SpaceRogue did you get what you need for the secret weapon?

Yup. Remember the ATM job I did in Osaka last October? She’ll be coming from a specialty shop I found there.

Should be a snap to clone the key card, once @SpaceRogue swipes it.

CEO of

Chicago, Illinois

LET’S ROLL.

READY, QT?

THIS BLOKE HAS BEEN RUNNING ERRANDS FOR THREE HOURS NOW. HE REALLY DOES EVERYTHING HIMSELF, JUST LIKE SNOW AND CHRIS RESEARCHED.

THAT’S STILL PICKING UP THE WI-FI PACKETS THAT THE CAR IS COMMUNICATING VIA GEOFENCING---PRESCRIPTION ORDERS, DINNER RESERVATIONS.

MOST OF THE DATA IS ENCRYPTED, THOUGH.

WAIT. I’M GETTING SOMETHING. AUTOMATIC TEXT MESSAGES ABOUT [REDACTED AND WHO’S THE COMPANY CREDENTIALS?

WE’LL NEED TO BE ON-SITE AT 10. GONNA GO TO GET INTO HIS CORPORATE ACCOUNT. I HOPE SNOW’S PLAN WORKS.
The next day.
Somewhere near HQ.

AND NOW FOR YOUR ACCESS KEYS.

NO, STEVE. YOU'RE FIRST.

BULMOG. IS THAT A NEEDLE?!!

SWIP.

IT SURE IS. I'VE BEEN LOOKING INTO IMPLANTABLE RFID CHIPS.

Q IS PROGRAMMING THEM WITH BUILDING ACCESS NOW.

DONUT THURSDAYS! YES!

I'LL ATTACK THE ONLINE RESERVATIONS SYSTEM AND SECURE THE CONFERENCE ROOM.

OKAY, STEPHEN. EVERYONE ELSE, USE THE CEO'S CREDENTIALS AND START DIGGING.

ON OUR LAST JOB, THE CLIENT THOUGHT ALL WE DID WAS STEAL AN ACCESS CARD.

IT CAN'T THINK OF A BETTER WAY TO MAKE APOINT.

MORNING!

TIKKITY TLAH TLAH

I'VE GOT THE MANUFACTURING DOCUMENTATION FOR THE AVG.
THAT CHECK THIS OUT.
During the build process, the vehicle's head unit wirelessly connects to an open access point to download the latest firmware. That's fine, except... except what?

I don't see anything about wiping the access point after the vehicles leave the factory. If the vehicle's still beaming...

-- we can become the network if seeking access to...

"We can go even further by the look of the chip design. The car itself can become a Wi-Fi hotspot. With the right malware, we could turn off critical safety features in every car of this model that comes into range with our infected Patient Zero."

I'll call Charles.

No way.
Several months later.

Says they’ve fixed the vulnerabilities in their building access and the AV. We’ll be testing their solutions starting next week.

Las Vegas, Nevada

Black Hat conference, NoSteve’s hotel room.

What the hell?!

"We’ve learned this: Always be on the lookout for a prank from your teammates."

Speaking of mission-critical work, we learned an important lesson from this engagement. One that videoman Space Rogue and EvilMao incorporated brilliantly in their recent deployment of a secret weapon at Black Hat.

This "lesson" was absolutely nothing to do with the job. Does it? Videoman?

Of course not.
"Of course, there's always the revenge prank..."
Writer **REGINA BEDIAKO @Epic Digital**
Regina Bediako has produced nonfiction print, web, TV and podcast features for publications like HuffPost and USA Today and for Vox Media. Epic Digital works with some of the world’s most respected companies to find and tell amazing true stories.

Artist **MADO PEÑA**
Mado Peña is a comic artist based in Barcelona, Spain. She’s best known as a colorist for her work at DC Comics’ Arrow, Dargaud’s Les Beaux Étés and, most recently, Panini’s Alma Cubrae.

Color **BRYAN VALENZA**
Bryan Valenza is a comic book colorist based in Jakarta, Indonesia. He currently occupies his time coloring projects that include Skies of Fire, InSEXts, Golgotha, Mighty Morphin Power Rangers, Witchblade and more.

Letters **ROB LEIGH**
Letterer Rob Leigh is a comics veteran with more than 25 years in the business under his belt. Over the course of his career, he’s been at the bottom of the sea with SpongeBob SquarePants, patrolled Gotham City’s rooftops with Batman and soared beyond our solar system with Superman.

Covers **ALEX ARIZMENDI, a.k.a. MFK00**
Alex Arizmendi, a.k.a. MFK00, is a graphic artist from Mexico City with more than 20 years of experience in the advertisement and entertainment fields, from comics to motion pictures. He was recently published by Marvel Comics and Aspen Comics, among others.

About X-Force Red
X-Force Red is an autonomous team of veteran hackers within IBM Security hired to break into organizations and uncover vulnerabilities that criminal attackers might exploit. X-Force Red offers penetration testing and vulnerability management programs to help security leaders identify and remediate flaws covering their entire digital and physical ecosystem.

X-Force Red can do whatever criminal hackers can do, but with the goal of helping security leaders strengthen their defenses and protect their most important assets.

Join the XFR team! View the latest job openings at X-Force Red.
https://www.ibm.com/security/services/x-force-red-team

Want to hire X-Force Red?
http://ibm.biz/xfrcomicbook

XFR Vol. 2
Coming Soon