THE WORLD’S DEADLIEST MALWARE

Chris Pogue, Director

Trustwave®
SMART SECURITY ON DEMAND
JUST KIDDING...CHANGE OF PLANS

You’ll really like this though...I promise...
STUPID HACKER TRICKS
TALES FROM THE FRONTLINES

Chris Pogue, Director / Grayson Lenik, Senior Security Consultant
This presentation represents the best of the worst encountered by Trustwave SpiderLabs Digital Forensics and Incident Response Team.

- Material additionally provided by Chris Hague, Lee Sult, Bryan Barnhart, Jon Spruill, and Melia Kelly (arguably the best DFIR team on this planet).
Stupid Hacker Tricks

Hacker Guerilla Black Pleads Guilty To Credit Card Fraud Scheme

by Yohance Kyles (@HUEYmixwitRILEY) July 10th, 2013 @ 4:47pm

Argentin Man A 19-year-old Miss Teen...

Fidel Salinas Jr.

without authorization, court records show.
Why do they get caught?

- Inexperience
- Bad luck
- Laziness/Drugs/Misplaced Trust
- Obvious footprint on systems
- Some of them are just plain dumb

- There are also some wicked smart security professionals and cops out there hunting them
Inexperience

Investigators can do that?

- Hacker 1 has a reseller deal with a medium size data hosting company and resells web servers as part of his development business.

- He has a falling out with the hosting company, demands some refunds and gets no satisfaction.
  - Decides to hack the hosting company and does so successfully via SQL injection
  - Starts changing database values and extending credit and server leases in the database
  - Problem is that he added the credits to his own, real account and continued to re-sell servers that he never paid for in the first place. Trustwave investigated, discovered all the evidence and turned the information over to law enforcement.
  - The original account that he added credit to contained his full name, current address, multiple phone numbers and billing information.

- “This is the only time I’ve ever done anything like this, I didn’t think anyone could track those kind of things”
Inexperienced

Investigators can do that?

- Disgruntled employee sets up back door remote access right before quitting.
- Uses that access to delete all of the active directory and email accounts after leaving.
  - LogMeIn account was registered using his personal email account
  - IP used to check email and delete the accounts was the same...his new employers address.
- Attack was against a law firm!
  - Lawyers won’t prosecute will they?
  - Currently undergoing federal prosecution
Bad Luck

- Hacking crew pops a restaurant Point of Sale system and installs keylogging software to capture credit card data.
- Hacking crew 2 compromises the same restaurant after crew 1 has installed a keylogger.
  - Crew 2 installs different malware on the systems while being keylogged, then identifies the keylogger and turns it off.
  - But...they leave the output file from the keylogger in place for us to find.
  - Output file contains ftp IP address, username, passwords and a full recording of them performing a malware install.

- Trustwave performs investigation, identifies jump server located in US from keylogs, informs LE. LE serves a Pen/Trace and identifies attacker source and numerous other victim systems. Jump box is shut down.
Laziness/Drugs/Misplaced trust

Will you Marry me???

- Hackers 1, 2, and 3 are holed up in a non-extradition country.
- Hacker 1 starts an online relationship with an extraordinarily attractive female...who happens to be a federal agent.
- Female Fed asks Hacker 1 to come to the US and visit her...she said that the trip would be WORTH it!
- Hacker 1 agrees...hit the tarmac...rushes into her “loving” arms, only to hear the clickty clacking of handcuffs.
- And the sweet words whispered into his ears, “You’re under arrest”.
- Hacker 1 informs Hackers 2 & 3 that he’s getting married.
- Hackers 2 & 3 come to the “wedding”, and are also arrested upon landing in the US.
Coast to Coast breach of a POS software company

- Hacker1 pops a POS software company and identifies all of their customers across the country.
- Successfully installs a keylogger at nearly every location in the country and engages Hacker2 to help sell credit card data.
- Trustwave performs investigation and uncovers a very tricky configuration file for the keylogger. Malware team reverse engineers the config file and supplies a decoder. Decoded log files all point to a hacked Windows dump server at a kindergarten in New Jersey.
  - LE is engaged
- LE serves a Pen/Trace on the dump server and identify all victims as well as an IP address to a home in the D.C. area.
Laziness/Drugs/Misplaced trust

Coast to Coast breach of a POS software company

- Home in D.C. is “raided” by the USSS and Hacker1 is arrested
  - They knocked on the door and identified themselves and the parents pointed towards the basement and say “He’s down there”.
  - Hacker1 has a terrible heroin problem and sells CC data to support his habit.
- Hacker1 rolls over on Hacker2 and agrees to give LE his logins and IRC creds.
- LE impersonates Hacker1 and gets Hacker2 to meet him “on vacation” in an extradition friendly country.
- Hacker 2 is arrested and rolls over on his biggest buyer.
Laziness/Drugs/Misplaced trust
System Footprint

Remember when?

- It wasn’t unusual for something like word to use 30% of the CPU and it was common to see a PC running at 85-90%?
- Nowadays even busy systems rarely spike out CPU usage

- What if an attacker added a routine to create a debug log and then continually scraped that debug log for CC data and added that data to another log which is then parsed and added to another log for exfiltration? What if that middle log was never cleared and continued to grow exponentially until the simple parsing with a regex ground the system to a halt?
“Our server ran out of space about 3 months ago so we added another drive”

- It’s out of space because there’s a memory dumper running 24/7 and dropping output in the root of C:\
- You bought your attacker a bunch of room to work
“I just installed a keylogger but I forgot it was there”

- Hacker installs keylogger, forgets some of his other tools and FTP’s out to get them. Then opens an IRC client and starts chatting with a hacker buddy and gives away his handle.
  - “Thanks again for the jump server creds and handle, Special Agent Secret Squirrel will take it from here”
Just Plain Dumb

“I just hacked a Government official I’m going to talk about in an open IRC channel.”

– Cuz there are no Feds watching those channels, right?

– “BTW thanks for confirming your other handles in the IRC channel, we know who you are in real life and we’ll see you at DEFCON”

Love,

THE FBI
Just Plain Dumb

SQL Injection FTW! ODBC connection - not so much

- Hacker compromises an online retailer via SQLi and successfully dumps the entire database out to a jump server through the use of an ODBC connection...
  - That he identifies in it’s entirety in the web logs for the intrusion.
  - IP address, port, username, password.
  - IP was a server in the US
Just Plain Dumb

“I plugged a physical keylogger into the front desk PC’s at your hotel”

- Then started making reservations with credit cards I stole from your other customers under my real name.
  - Also made a late check-in reservation every time I come in to collect data from the devices
  - One night the Secret Service was hidden in the lobby waiting...
After a “knock” on the front door of a hackers apartment, he ran to the balcony to discard a laptop from 31 stories up.

Not a bad plan, except that it landed in the grass and the hard drive still powered up and spun just fine.
Just Plain Dumb

Knock-knock
Just Plain Dumb

Laptop Overboard
I’m Houdini

- Once in custody, hacker attempts to “pick” his way out of the interrogation room with a piece of zip-tie, while he’s being videoed through the one-way glass...sigh
Malware authors

- A malware author embedded the following comment into his malware:
  - "DEAR WHITEHATS: This bot isn't protected because I'm lazy and you're not going to do anything anyway, not because I'm inept. Although I have added a dirty cipher to please you. Come chat with us, we're friendly."

- Multiple cases with brand new malware or variants with hard coded IP’s and credentials. They don’t last long.
Conclusion

- Hacking is not magic. Everything leaves a trace, the real trick is knowing where to look.

- Hackers are real people with real flaws. They are most definitely not unstoppable super humans.

- Be proactive, test your organizations, have a plan, and *keep some danged logs!*
Thank you!