Home Invasion v2.0

WHO ARE WE?

The Presenters

Daniel “unicornFurnace” Crowley
- Managing Consultant, Trustwave SpiderLabs

Jennifer “savagejen” Savage
- Software Engineer, Tabbedout

David “videoman” Bryan
- Security Consultant, Trustwave SpiderLabs

WHAT ARE WE DOING HERE?

The “Smart” Home

Science fiction becomes science fact

Race to release novel products means poor security

Attempt to hack a sampling of “smart” devices

Many products we didn’t cover

- Android powered oven
- Smart TVs (another talk is covering one!)
- IP security cameras

WHAT'S OUT THERE?

Belkin WeMo Switch

Belkin WeMo Switch

1. Vulnerable libupnp version
2. Unauthenticated UPnP actions
    1. SetBinaryState
    2. SetFriendlyName
    3. UpdateFirmware

MiCasaVerde VeraLite

MiCasaVerde VeraLite

1. Lack of authentication on web console by default
2. Lack of authentication on UPnP daemon
3. Path Traversal
4. Insufficient Authorization Checks
    1. Firmware Update
    2. Settings backup
    3. Test Lua code
5. Server Side Request Forgery
6. Cross-Site Request Forgery
7. Unconfirmed Authentication Bypass
8. Vulnerable libupnp Version

INSTEON Hub


My Bayshore Office
Update Status
ON
Guest room
OFF
ON
Aquariums
OFF

INSTEON Hub

1. Lack of authentication on web console
    1. Web console exposed to the Internet

Karotz Smart Rabbit

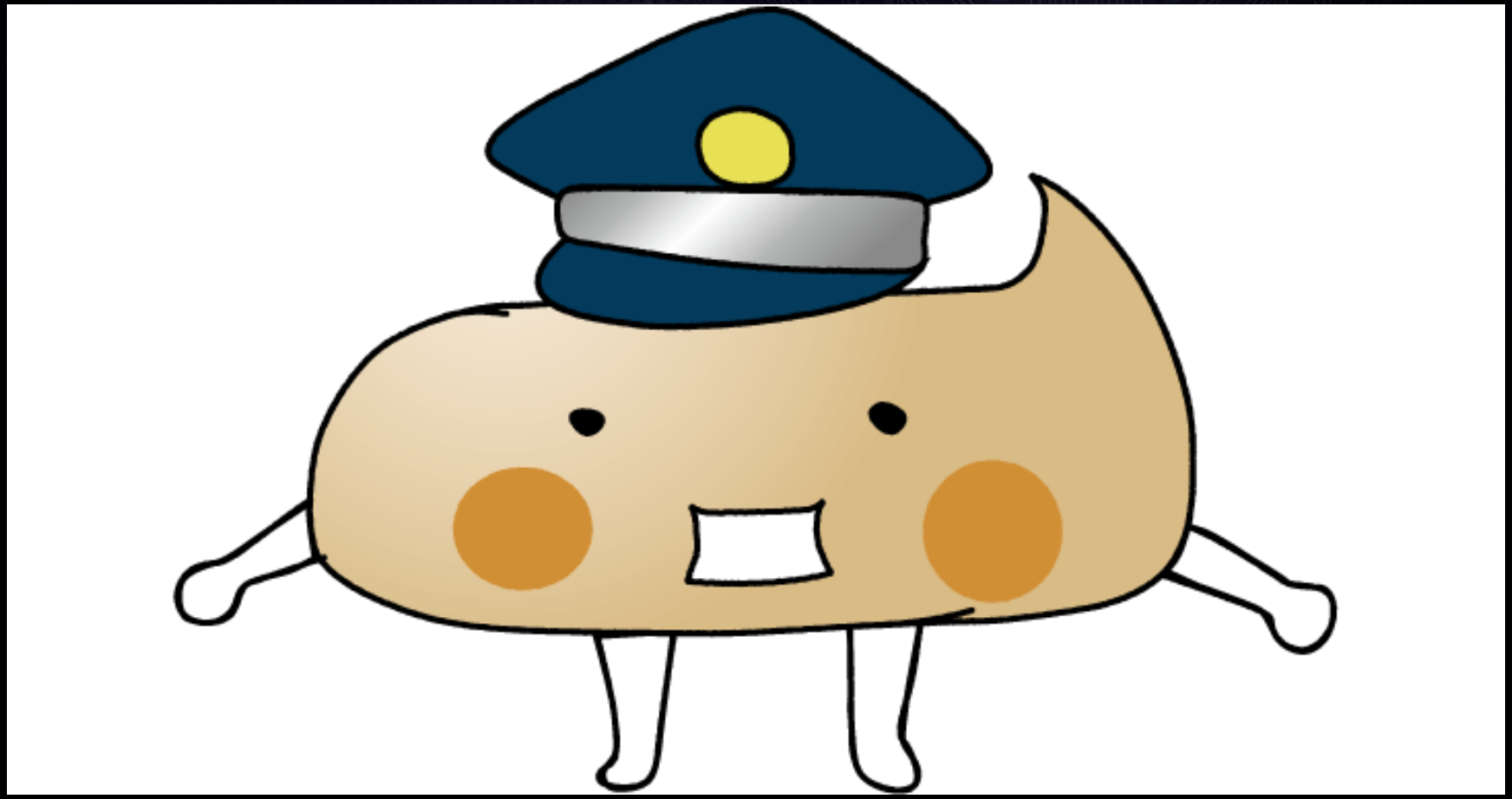
Karotz Smart Rabbit

1. Exposure of wifi network credentials unencrypted
2. Python module hijack in wifi setup
3. Unencrypted remote API calls
4. Unencrypted setup package download

Linksys Media Adapter

1. Unauthenticated UPnP actions

LIXIL Satis Smart Toilet



LIXIL Satis Smart Toilet

1. Default Bluetooth PIN

Radio Thermostat

1. Unauthenticated API
2. Disclosure of WiFi passphrase

SONOS Bridge

SONOS Bridge

1. Support console information disclosure

DEMONSTRATION

CONCLUSION

Questions?

Daniel “unicornFurnace” Crowley
dcrowley@trustwave.com
@dan_crowley
Jennifer “savagejen” Savage
savagejen@gmail.com (PGP key ID 6326A948)
@savagejen
David “videoman” Bryan
dbryan@trustwave.com
@_videoman_