GitHub - MRGEffitas/Ironsquirrel: Encrypted exploit delivery for the masses

By MRGEffitas

Archived: 2026-04-05 23:14:04 UTC

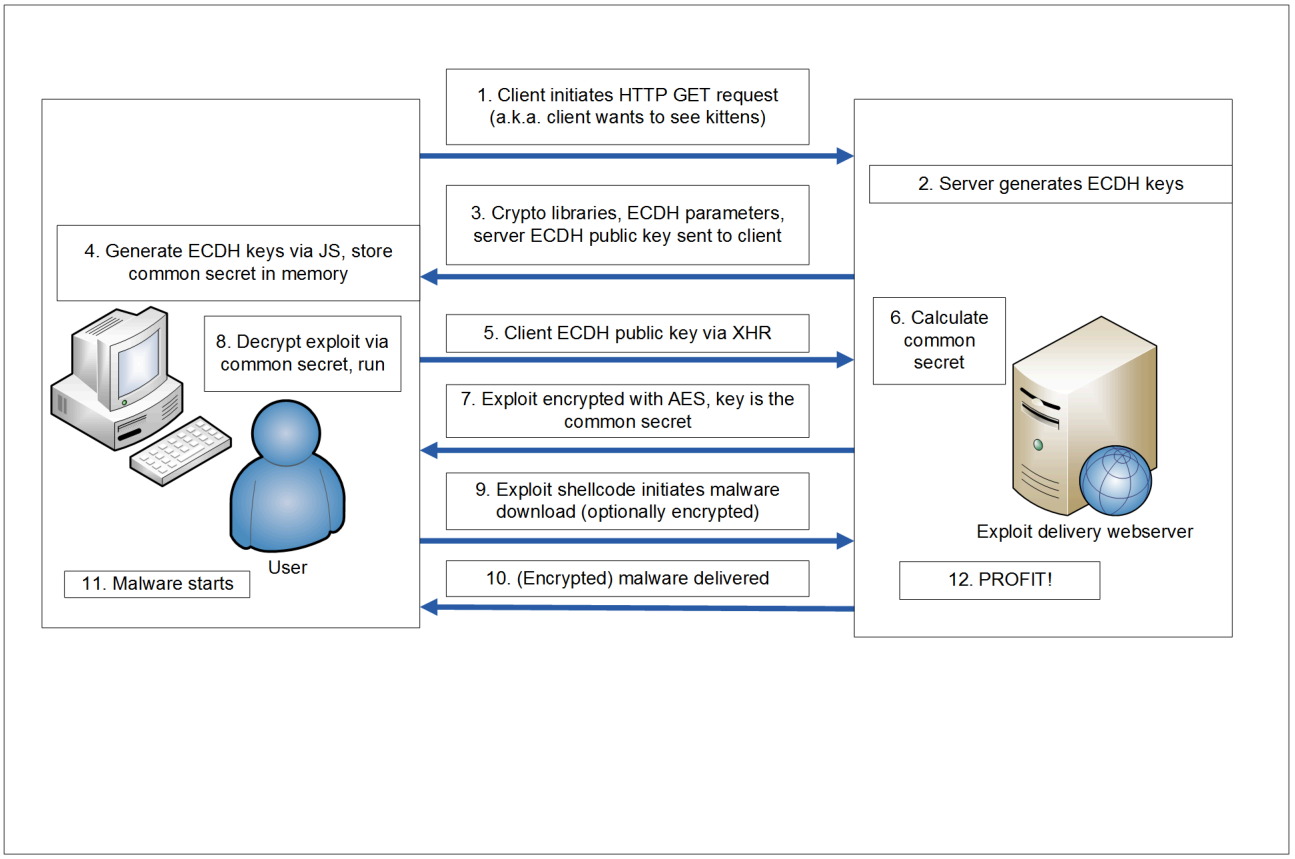
This project aims at delivering browser exploits to the victim browser in an encrypted fashion. Ellyptic-curve Diffie-Hellman (secp256k1) is used for key agreement and AES is used for encryption.

By delivering the exploit code (and shellcode) to the victim in an encrypted way, the attack can not be replayed. Meanwhile the HTML/JS source is encrypted thus reverse engineering the exploit is significantly harder.

If you have no idea what I am talking about, Google for "How to hide your browser 0-days", and check my presentation. Or check out it on Youtube: https://www.youtube.com/watch?v=eyMDd98uljI Or slides on Slideshare: https://www.slideshare.net/bz98/how-to-hide-your-browser-0days

The idea of encrypted exploit delivery was first published by me in June 2, 2015: https://twitter.com/zh4ck/status/605754804472823808 https://www.mrg-effitas.com/research/generic-bypass-of-next-gen-intrusion-threat-breach-detection-systems/

The Angler exploit kit guys just stole my idea. And implemented it poorly.



Getting Started

These instructions will get you a copy of the project up and running on your local machine for development and testing purposes.

Prerequisites

Mandatory dependencies - clone the IRONSQUIRREL project, cd into the project directory, and run the following commands:

```
 sudo apt-get install ruby-dev
bundle install
```

Actually nokogiri and gibberish gems will be installed.

Optional dependency (for Powershell based environment aware encrypted payload delivery): Ebowla
https://github.com/Genetic-Malware/Ebowla

Installing

1. Clone the IRONSQUIRREL project
2. Install the prerequisites
3. (Optional) Edit IRONSQUIRREL.rb
    1. Change the listen port
    2. If Ebowla is used, configure the paths
4. (Optional) If Ebowla is used, configure genetic.config.ecdh in the Ebowla install directory
5. Run IRONSQUIRREL.rb

```
ruby IRONSQUIRREL.rb --exploit full_path_to_exploit
```

Example

```
ruby IRONSQUIRREL.rb --exploit /home/myawesomeusername/IRONSQUIRREL/exploits/alert.html
```

After that, visit the webserver from a browser. Example output:

```
 Listening on 2345
GET / HTTP/1.1
GET /sjcl.js HTTP/1.1
GET /dh.js HTTP/1.1
GET /client_pub.html?cl=SOifQJetphU2CvFzZl239nKPYWRGEH23ermGMszo9oqOgqIsH5XxXi1vw4P4YFWDqK6v4o4jIpAVSNZD1x5NTw%3
GET /final.html HTTP/1.1
```

```
GET /sjcl.js HTTP/1.1
The end
```

Deployment instructions for production environments

1. Let me know if you use this for real
2. Spend at least 2 weeks to figure out what could go wrong

Contributing

Feel free to submit bugfixes, feature requests, comments ...

Authors

- **Zoltan Balazs (@zh4ck)** - *Initial work*

License

This project is licensed under the GPL3 License - see the LICENSE.md file for details

Acknowledgments

- @CrySySLab
- @SpamAndHex
- @molnar_g
- @midnite_runr
- @buherator
- @sghctoma
- @zmadarassy
- @xoreipeip
- @DavidSzili
- @theevilbit
- Szimeus

Source: https://github.com/MRGEffitas/Ironsquirrel