Tracking Actors using Banking Malware through their Webinfects

James Wyke
Principal Security Researcher
Agenda

- Introduction
- What are WebInjests?
- Current Banking Malware and WebInjests
- Capabilities of WebInjests
- Tracking Actors Across Malware Families
- Conclusion
Introduction
Introduction

Who Am I?

- I am
  - Principal Security Researcher, FireEye Threat Intelligence

- I do
  - RE
  - Write code
  - Botnet monitoring
  - Banking malware
  - Webinjects
What are WebInjests?
What are WebInjests?

- WebInjests are a feature of Banking Malware where code is injected into a webpage.
- Ranging from simple form field additions to full blown Automated Transfer Systems.
- Injected code frequently just stub code.
- WebInjests often run as their own web application with Administration Panel.
  - Web Injests System (ATS).
- Injects sold through forums, often work with multiple malware families, or injects formats – Zeus vs Gozi.
- Some systems in circulation for many years.
Current Banking Malware and WebInjests
Current Banking Malware and WebInjests

- **Trickbot** - High prevalence, wide geographic targeting
- **Dridex** - High prevalence, mostly targeting North America
- **ISFB** - High prevalence, wide geographic targeting, many variants and actors
- **Danabot** - Moderate prevalence, moderate geographic targeting, multiple customers
- **Gootkit** - Moderate prevalence, moderate geographic targeting, multiple affiliates
- **Ramnit** - Moderate prevalence, limited geographic targeting, multiple customers
- **IcedID** - Moderate prevalence, mostly targeting North America
- **Qakbot** - Moderate prevalence, mostly targeting North America
Capabilities of WebInjects
Capabilities of WebInjests

Grabbers

- “Grab” victim data from the targeted web site
  - Login, password + other credentials
  - Payment card data – cc, exp, cvv, pin
  - PII – name, SSN, DOB, address

- Capture data that already exists on the page, or elicit further information
  - Record login credentials
  - Scrape data from account page
  - Inject code to ask further questions
Capabilities of WebInjects

Automated Transfer Systems and Replacers

▪ Automated Transfer System (ATS)
  – Fully automated process for transferring money out of victim account
  – Auto-calculates amount
  – Auto-selects mule account
  – Uncommon

▪ Hybrid automated and manual transfer
  – Combines automated components with manual actions, e.g. hijack genuine transfer with attacker account number, hide evidence from victim; social engineer TAN code

▪ Replacer
  – Replace attacker transfers in UI
Capabilities of WebInjests

Others

- Cryptocurrency miners
  - Variant of “authedmine” code injected
- Email manipulation
  - Inject payload into email chain
- Maintain session
  - Prevent genuine logout
  - Allows attacker to piggy back the existing session
- Trigger other Bot actions
  - Initiate VNC session, start screengrab/recording of browser
Tracking Actors Across Malware Families
Tracking Actors Across Malware Families

WebInjests Infrastructure

- The WebInjests have their own infrastructure which we can track
- URLs, Domains, IPs embedded in injected code
- URLs show up in WebInjests from multiple malware families
https://clientdomain.info/c/lucifer/us/amzats

https://managertrafficdirect.pw/api/cpanel/t.js

https://lio.party/kenta/in/relaxbanking/rel.php?id=%BOTID%
Chanitor Payloads
Emotet Payloads
Conclusion
Conclusion

- Many active malware families deploying WebInjests

- Impact can be severe – financial loss, data loss

- Actors use the same WebInjests across multiple malware families
Thank You